MEMORANDO	
Código Depend.:	**2310300**
Para:	**WILLIAM LIBARDO MENDIETA MONTEALEGRE DESPACHO DE LA SECRETARIA JURIDICA DISTRITAL MAGDA MERCEDES ARÉVALO ROJAS OFICINA ASESORA DE PLANEACION EDGAR ENRIQUE OVALLE CUERVO OFICINA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES**
De:	**OFICINA DE CONTROL INTERNO**
Asunto:	**INFORME DE SEGUIMIENTO AL PLAN DE SOSTENIBILIDAD DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG Y MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SJD**

Referenciado(s)	N/A

Respetado doctor Mendieta:

En cumplimiento del Plan Anual de Auditoría 2022, de manera atenta remito el informe de "Seguimiento al Plan de Sostenibilidad del Modelo Integrado de Planeación y Gestión MIPG- y el anexo 1 Informe de Seguimiento al Modelo de Seguridad y Privacidad de la Información", de la Secretaria Jurídica Distrital, con fechas de corte 31 de marzo y 25 de abril de 2022, respectivamente.

Este informe se da a conocer al señor Secretario en cumplimiento de los dispuesto en el artículo 648 de 2017 –Artículo 16 "*Adiciónese el Capítulo 4 del Título 21, Parte 2, Libro 2 del Decreto 1083 de 2015, los siguientes artículos: (…) Parágrafo 1. Los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal al representante legal de la entidad y al Comité de Coordinación de Control Interno y/o comité de auditoría y/o junta directiva, y deberán ser remitidos al nominador cuando éste lo requiera*".

Así mismo este seguimiento se remite a la Oficina de Tecnologías de la Información y de las Comunicaciones y a la Oficina Asesora de Planeación, para los fines pertinentes.

Atentamente,

CAROLINA LOZANO ARDILA

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

c.c.e.:
Anexo: N/A
Anexos Digitales: 3

Proyectó: ZULMA YANET GOMEZ PERALES-OFICINA DE CONTROL INTERNO
Revisó: CAROLINA LOZANO ARDILA-OFICINA DE CONTROL INTERNO | CAROLINA LOZANO ARDILA-OFICINA DE CONTROL INTERNO |
Aprobó: CAROLINA LOZANO ARDILA-OFICINA DE CONTROL INTERNO

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Informe de seguimiento al Plan de Sostenibilidad del Modelo Integrado de Planeación y Gestión MIPG

PRIMER TRIMESTRE 2022

Oficina de Control Interno

Fecha elaboración, junio de 2022

1. OBJETIVO

Realizar el seguimiento de las actividades establecidas en las políticas que hacen parte del Plan de Sostenibilidad del Modelo Integrado de Planeación y Gestión MIPG de la Secretaría Jurídica Distrital. Así mismo realizar análisis del Modelo de Seguridad y Privacidad de la Información en lo que respecta a los controles administrativos y Ciclo PHVA

2. ANTECEDENTES

Plan de Sostenibilidad de MIPG

Mediante los memorandos 3-2021-8901, 3-2021-8917, 3-2021-8919, 3-2021-8920 y 3-2021-8921 del 30 de noviembre de 2021, la Oficina Asesora de Planeación solicitó a algunas dependencias de la Secretaria Jurídica Distrital, la definición de actividades del Plan de Sostenibilidad MIPG de la vigencia 2022, a lo cual se dio respuesta a través de los memorandos 3-2021-9099 del 7 de diciembre de 2021 (oficina TICS), 3-2021-9279 del 15 de diciembre de 2021 (Dirección Distrital de Política Jurídica).

Por medio del memorando 3-2022-2285 del 24 de marzo de 2022, la Oficina Asesora de Planeación solicito el reporte de avance del Plan de Sostenibilidad MIPG 2022 correspondiente al primer trimestre de la vigencia, a lo cual las dependencias requeridas dieron respuesta mediante memorandos 3-2022-2674 (Dirección Distrital de Política Jurídica), 3-2022-2703 (Dirección de Gestión Corporativa), 3-2022-2717 (Oficina de Control Interno), 3-2022-2819 (Dirección Distrital de Inspección Vigilancia y Control), y 3-2022-3341 (Oficina TICS).

El presente seguimiento con fecha de corte 31 de marzo de 2022, se realiza con base a la información enviada por la Oficina Asesora de Planeación, mediante memorando 3-2022-2517 de fecha 25 de mayo de 2022, asunto: Respuesta al comunicado 3-2022-3393 Solicitud de información plan de sostenibilidad del modelo integrado de planeación y gestión.

3. MARCO NORMATIVO

- Artículo 133, Ley 1753 de 2015 *"Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país"*: "Integración de Sistemas de Gestión. Intégrense en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad de qué trata la Ley 872 de 2003 y de Desarrollo Administrativo de que trata la Ley 489 de 1998.

- Capítulo 3 Modelo Integrado de Planeación y Gestión, del Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".

- Marco General del Modelo Integrado de Planeación y Gestión, Versión 4, marzo 2021.

- Decreto Distrital 807 de 2019 “Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones”.

- Manual de Gobierno Digital, implementación de la política de Gobierno Digital (Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) emitido por el Ministerio de Tecnología de la Información y las Comunicaciones, versión 6 diciembre 2018.

- Lineamientos técnicos de gestión del conocimiento y la innovación V1 de 2020, expedido por el Departamento Administrativo de la Función Pública.

4. CRITERIOS Y METODOLOGÍA DEL SEGUIMIENTO.

- Revisión de actividades, metas y productos previstos en el Plan de Sostenibilidad del Modelo Integrado de Gestión 2022, tomando como base el cronograma definido.
- Revisión de las evidencias reportadas por la Oficina Asesora de Planeación, mediante memorando 3-2022-2517 de fecha 25 de mayo de 2022
- Verificación en página web de la Secretaría Jurídica y demás sistemas de información.
- Análisis detallados de las políticas de gobierno digital y gestión del conocimiento y de la innovación.

Hace parte del presente informe el siguiente anexo:

Anexo 1. Informe de Seguimiento Modelo de Seguridad y Privacidad de la Información de la Secretaria Jurídica Distrital, corte 25 de abril de 2022.

5. DEPENDENCIAS RESPONSABLES DEL PROCESO

Las dependencias que tienen a su cargo la ejecución de actividades del Plan de Sostenibilidad de MIPG 2022 son: Dirección de Gestión Corporativa, Dirección Distrital de Inspección Vigilancia y Control, Dirección Distrital de Política Jurídica, Oficina Asesora de Planeación, Oficina de Tecnología de la Información y las Comunicaciones y Oficina de Control Interno.

6. SEGUIMIENTO A LAS POLÍTICAS INCLUIDAS EN EL PLAN DE SOSTENIBILIDAD DE MIPG 2022

El seguimiento se efectuó a las actividades establecidas en las veintidós (22) políticas definidas en el Plan de Sostenibilidad del Modelo Integrado de Planeación y Gestión, de acuerdo con la siguiente matriz:

Dimensión	Política	Actividades programadas 2022
Talento Humano	Gestión Estratégica del Talento Humano	27
	Integridad	45
	Conflicto de intereses	19
	Planeación Institucional	16

Dimensión	Política	Actividades programadas 2022
Direccionamiento Estratégico y Planeación	Compras y Contratación Publica	1
	Plan Anticorrupción y Atención al Ciudadano.	15
Gestión con valores para resultados	Gobierno Digital	71[1]
	Seguridad Digital	44
	Fortalecimiento Organizacional y Simplificación de Procesos	1
	Servicio al Ciudadano	62
	Defensa Jurídica	8
	Componente Ambiental	12
	Participación Ciudadana	28
	Rendición de Cuentas	101
	Racionalización de Trámites	46
Evaluación de Resultados	Seguimiento y Evaluación del Desempeño.	21
Información y Comunicación	Transparencia y Acceso a la Información y Lucha Contra la Corrupción	49
	Gestión Documental	115
	Gestión de la Información Estadística	31
Gestión del conocimiento y la innovación	Gestión del Conocimiento y la Innovación.	50
Control Interno	Control Interno	9

Fuente: Plan de Sostenibilidad MIPG 2022, Cálculos propios.

6.1. Política Gestión Estratégica del Talento Humano

Estado actividades	Total
Cumplidas	8
En ejecución	1
Sin inicio en primer trimestre	18

Fuente: Plan de Sostenibilidad MIPG 2022 – Política Gestión estratégica de Talento Humano, Cálculos propios

6.2. Política de Integridad

Estado actividades	Total
Cumplidas	10.25
En ejecución	0
Sin inicio en primer trimestre	7.75

Fuente: Plan de Sostenibilidad MIPG 2022 – Política Integridad, Cálculos propios

6.3. Política de Conflicto de intereses.

Estado actividades	Total
Cumplidas	10.25
En ejecución	0
Sin inicio en primer trimestre	7.75

Fuente: Plan de Sostenibilidad MIPG 2022 – Política Conflicto de Intereses, Cálculos propios

[1] Resultado de la revisión de la política de Gobierno Digital, se logró establecer setenta y un (71) actividades previstas con producto determinado. Se observó formulación de acciones sin producto concreto, en construcción o que de acuerdo a lo definido por el área no requieren desarrollo en 2022 y tienen programación, el detalle del análisis de la política se encuentra descrito en el numeral 6.8 del presente informe.

Para esta política se observa la definición de la misma actividad dos veces, la cual se encuentra relacionada a dos actividades de gestión diferentes, una para servidores públicos y otra para contratistas, para lo cual se recomienda formularlas de manera independiente de forma que quede claro lo que se va a medir, ya que tanto los logros, como resultados y evidencias deben ser diferentes.

Adicionalmente, no se adjuntaron evidencias que den cuenta de la ejecución a 31 de marzo de 2022 de las actividades anteriormente mencionadas. Sin embargo, mediante correo electrónico de fecha 21 de junio de 2022, el proceso de talento humano aclara que 113 contratistas realizaron el diligenciamiento de la declaración de bienes y rentas y conflicto de intereses.

Así mismo, es importante que se precise si la medición se realizará para el diligenciamiento a inicios de cada contrato, para el caso de contratistas o en la actualización que se debe realizar entre los meses de junio y julio.

6.4. Política de Planeación Institucional

Estado actividades	Total
Cumplidas	9
En ejecución	0
Sin inicio en primer trimestre	7

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Planeación Institucional, Cálculos propios

Se evidenció que las actividades programadas en el primer trimestre 2022, se ejecutaron acorde a su descripción y tiempos establecidos en el Plan de Sostenibilidad de MIPG 2022.

6.5. Política de Compras y Contratación Pública

Estado actividades	Total
Cumplidas	0
En ejecución	0
Sin inicio en primer trimestre	1

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Compras y Contratación Pública, Cálculos propios

Se observó que no se realizó programación de actividades durante el primer trimestre de 2022.

6.6. Plan anticorrupción y Atención al Ciudadano

Estado actividades	Total
Cumplidas	5
En ejecución	0
Sin inicio en primer trimestre	10

Fuente: Plan de Sostenibilidad MIPG 2022 – Plan anticorrupción y Atención al Ciudadano, Cálculos propios

Respecto a la actividad “Presentar y aprobar en el Comité MIPG el PAAC y el mapa de riesgos de corrupción”, no se aportó el Acta del Comité de Gestión y Desempeño Institucional en donde se realizó dicha aprobación. Sin embargo, estos informes se encuentran publicados en la página web de la SJD.

6.7. Política de fortalecimiento organizacional y simplificación de procesos

Estado actividades	Total
Cumplidas	0
En ejecución	0
Sin inicio en primer trimestre	1

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de fortalecimiento organizacional y simplificación de procesos, Cálculos propios

Se evidenció que la política en el Plan de Sostenibilidad de MIPG, no tiene actividades programadas para el primer trimestre de 2022.

6.8. Política de Gobierno Digital

Estado actividades	Total
Cumplidas	42
Actividades para revisión	**152**
Sin inicio en primer trimestre	29

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Gobierno Digital, Cálculos propios

Se evidenció que treinta y siete (37) actividades que se encontraban programadas para el segundo trimestre, se ejecutaron en el primer trimestre de 2022, relacionadas con las solicitudes de publicación por parte del Web Máster en la página web enlace transparencia y acceso a la información pública.

Se observó que ciento cincuenta y dos (152) actividades descritas en la columna “actividades resultado esperado”, no son actividades sino comentarios relacionados con el ítem del autodiagnóstico. No reflejan una actividad a ejecutar. Sin embargo, se observó su programación en el plan de sostenibilidad de la política analizada. Algunos de los comentarios se relacionan a continuación:

1. Se desarrolla la versión preliminar del documento, sin embargo, se espera que MINTIC se pronuncie frente a los cambios normativos los cuales fueron mencionados en reunión de nov de 2021 con el fin de ajustar el documento y aprobarlo en comité
2. Se validará la pertinencia y necesidad de actualización documental ya sea por obsolescencia técnica o necesidad jurídica
3. En la actualidad la entidad cuenta con procesos de gestión TI, sin embargo, se validará la pertinencia y necesidad de actualización documental ya sea por obsolescencia técnica o necesidad jurídica
4. La entidad cuenta con los esquemas de gobierno de tecnologías de la información e Instancias o grupos de decisión de TI definidas mediante comité MIPG, por lo cual no requiere actualización para el año 2022
5. Fichas de proyectos de Actos administrativos, resoluciones, certificaciones, Micrositio doctrina distrital, etc
6. En la actualidad la entidad cuenta con metodologías para gestión de proyectos TI, sin embargo, se validará la pertinencia y necesidad de actualización documental ya sea por obsolescencia técnica o necesidad jurídica
7. La entidad cuenta con herramientas para el seguimiento como matrices de riesgos, proyect charter, cronogramas, etc

8. Está en construcción
9. En la actualidad la entidad cuenta con el diseño de la arquitectura de LegalBog, y plantilla de arquitectura para sistemas backend, sin embargo, se validará la pertinencia y necesidad de actualización documental ya sea por obsolescencia técnica o necesidad jurídica
10. En la actualidad la entidad cuenta con proceso de calidad de datos, sin embargo, se validará la pertinencia y necesidad de actualización documental ya sea por obsolescencia técnica o necesidad jurídica

Adicionalmente, hay otras actividades incluidas en el plan de Sostenibilidad que presentan las mismas características. Por lo anterior, es necesario realizar la verificación, análisis de pertinencia y actualización de las mismas en el plan.

Respecto a la actividad “La entidad cuenta con los esquemas de gobierno de tecnologías de la información e Instancias o grupos de decisión de TI definidas mediante comité MIPG, por lo cual no requiere actualización para el año 2022”, se observó que el entregable es “1 documento”, sin embargo, la descripción de la actividad refiere que no es necesario su actualización. Por lo tanto, se recomienda que las actividades consignadas en el resultado esperado sean consistentes con la programación trimestral y la magnitud entregable.

Adicionalmente, se evidenció una actividad resultado esperado “en construcción”, lo no permite medir la actividad descrita ya que no se entiende cual es el resultado esperado "Está en construcción".

Análisis de la política de gobierno Digital

Se realizó evaluación de la política de Gobierno digital, de acuerdo con los componentes establecidos en el Manual de Gobierno Digital, implementación de la política de Gobierno Digital (Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) emitido por el Ministerio de Tecnología de la Información y las Comunicaciones, versión 6 diciembre 2018.

Teniendo en cuenta el esquema institucional planteado en el Manual de Gobierno Digital, se debe revisar la posibilidad de crear el Grupo de Arquitectura Empresarial, como apoyo para la toma de decisiones técnicas y operativas.

En cuanto al habilitador de los servicios de ciudadano digital, se debe establecer, cuáles son los servicios ciudadanos básicos que se van a generar, teniendo en cuenta lo establecidos en la sección 1 generalidades de los servicios ciudadanos digitales del Decreto 1413 de 2017, "Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015.

6.9. Política de Seguridad Digital

Estado actividades	Total
Cumplidas	15

En ejecución	0
Sin inicio en primer trimestre	29

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Seguridad Digital, Cálculos propios

Se observó de 44 actividades previstas para 2022, la ejecución de 15, algunas a pesar de tener programación en segundo semestre.

En los casos tales como el Plan Estratégico de Seguridad de la Información y el Plan de tratamiento de riesgos de Seguridad de la Información, su planeación sea acorde a los tiempos establecidos en el Decreto 612 de 2018

Adicionalmente, se observó que la frecuencia de la ejecución de las actividades descritas en la columna actividades - resultado esperado no es consistente con la programación trimestral registrada, tal como se observa a continuación:

ACTIVIDADES - RESULTADO	NOMBRE DEL RESPONSABLE	MAGNITUD ENTREGABLE	PROGRAMACIÓN TRIMESTRAL			
			1er trimestre	2do trimestre	3er trimestre	4to trimestre
Se realizarán 2 ejercicios de phising controlado en el año 2022 (cada semestre se realizará un ejercicio)	Leonardo Santos	1 Documento	0	1	0	0
Se identificarán los riesgos de seguridad digital a los activos de información críticos y cuya actividad se realizará en el segundo semestre del año 2022	Leonardo Santos	1 Documento	0	1	0	0
Todos los meses del año 2022 se realizará las actividades de identificación y planes de mitigación de vulnerabilidades técnicas en la infraestructura de la SJD	Leonardo Santos	1 Documento	0	1	0	0

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Seguridad Digital.

Para las siguientes actividades – resultados esperados, se observa reporte de avance del 25%, sin embargo, en el contenido del seguimiento reportado se indica cualitativamente que la actividad ya se realizó, por lo tanto, no es consistente la actividad, con la programación y el avance reportado a primer trimestre.

Es importante que se revisen las actividades – resultado, toda vez que cómo están definidas no permiten establecer claramente qué es lo que la entidad va a ejecutar en la vigencia, asociada a los lineamientos de la política.

ACTIVIDADES - RESULTADO ESPERADO	NOMBRE DEL RESPONSABLE	MAGNITUD ENTREGABLE /UNIDAD DE MEDIDA	PROGRAMACION TRIMESTRAL				AVANCE I TRIMESTRE	AVANCE LINEAMIENTO 2022
			1er trimestr	2do trimestr	3er trimestr	4to trimestr	AVANCE FÍSICO	
Los factores han sido identificados y están incorporados en los factores externos de la Entidad. Están aprobados por la Alta Dirección	Leonardo Santos	1 Documento	0	1	0	0	Los riesgos de seguridad digital ya fueron identificados, aprobados y formalizados en el sistema SMART de acuerdo con la metodología establecida por el DAFP (versión 5	25%
Los factores han sido identificados y están incorporados en los factores externos de la Entidad. Están aprobados por la Alta Dirección	Leonardo Santos	1 Documento	0	1	0	0	Los riesgos de seguridad digital ya fueron identificados, aprobados y formalizados en el sistema SMART de acuerdo con la metodología establecida por el DAFP (versión 5	25%
Para el año 2022 se ha realizado la contratación de un profesional para soportar las actividades del MSPI en la Entidad	Leonardo Santos	1 Documento	0	1	0	0	En el año 2022 se realizó la contratación del Ing. Leonardo Santos con el fin de realizar las actividades de cumplimiento del MSPI y seguridad digital en la entidad	25%
Para el año 2022 se ha realizado la contratación de un profesional para soportar las actividades del MSPI en la Entidad	Leonardo Santos	1 Documento	0	1	0	0	En el año 2022 se realizó la contratación del Ing. Leonardo Santos con el fin de realizar las actividades de cumplimiento del MSPI y seguridad digital en la entidad	25%
En el primer semestre de 2022 se revisará nuevamente en el SMART la documentación etiquetada para verificar si se necesita actualización	Leonardo Santos	1 Documento	0	1	0	0	En el mes de marzo se realizó revisión y actualización del etiquetado de políticas, manuales, planes, formatos y otros documentos en SMART	25%

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Seguridad Digital.

En el anexo No. 1 se adjunta el informe de seguimiento del Modelo de Seguridad y Privacidad de la Información de la SJD, en donde se pudieron verificar los avances y actividades detalladas en la autoevaluación con corte a abril de 2022 remitido por la Oficina de TICS, desde la Oficina de Control Interno se han realizado las principales recomendaciones teniendo en cuenta la información verificada.

Respecto a los controles administrativos objeto de análisis, se observó que los definidos en A5, A6, A7, A8, A17, A18 y A15, presentaron en su mayoría un avance significativo, teniendo en cuenta el diagnóstico aplicado en diciembre de 2019.

Por otro lado, y teniendo en cuenta los avances del ciclo PHVA por componentes desde la vigencia 2019 a 2022, se evidencia un mayor porcentaje de avance en dos componentes: Evaluación de desempeño y Mejora continua con un incremento del 20% para cada uno. El componente implementación presentó un avance del 16% y el componente de planificación presentó un avance del 10% siendo el menor avance desde la vigencia 2019 a 2022. En términos generales se presentó desde la vigencia 2019 a 2022, un porcentaje de incremento de avance del 66%, pasando del 32% al 98% con el ultimo corte al 25 de abril de 2022.

6.10. Política de Defensa Jurídica

Estado actividades	Total
Cumplidas	1
Sin ejecutar	1

En ejecución	0
Sin inicio en primer trimestre	6

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Defensa Jurídica, Cálculos propios

Respecto a la actividad "Mejorar la gestión contractual de la entidad, especialmente el ejercicio de planeación y supervisión de contratos", se reporta en el seguimiento que para el primer trimestre se realizó una actividad de gestión del conocimiento sobre el plan de acción, sin embargo, no se reportaron evidencias de dicha actividad, por lo que se incluye en la categoría "sin ejecutar".

6.11. Política de Servicio al Ciudadano

Estado actividades	Total
Cumplidas	10
Sin ejecutar	2
En ejecución	0
Sin inicio en primer trimestre	50

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Servicio al Ciudadano, Cálculos propios

Respecto a la actividad Encuesta de percepción ciudadana 2022, no se adjuntaron evidencias que sustenten la ejecución de la actividad para el primer trimestre de 2022.

En relación con la actividad "Expedir actos administrativos para decretar el Desistimiento Tácito de las PQRS que así lo requieran en cumplimiento de lo establecido en el procedimiento 2311000-PR-014 Gestión y Seguimiento a los Requerimientos Presentados por la Ciudadanía", no se aportaron las evidencias que den cuenta de los actos administrativos de declaratoria de desistimiento tácito de los dos (2) peticiones en estado "cerrado por desistimiento tácito" durante el primer trimestre de 2022.

6.12. Política de Racionalización de Trámites

Estado actividades	Total
Cumplidas	3
En ejecución	0
Sin inicio en primer trimestre	43

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Racionalización de Tramites, Cálculos propios

Se evidenció que las actividades programadas para el primer trimestre de 2022, de la política de racionalización de trámites, se ejecutaron y soportaron acorde al resultado esperado, entregable y programación trimestral establecida en el Plan de Sostenibilidad.

6.13. Política de Participación Ciudadana

Estado actividades	Total
Cumplidas	19
En ejecución	0
Sin inicio en primer trimestre	9

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Participación Ciudadana, Cálculos propios

Se evidenció que las actividades programadas para el primer trimestre de 2022, de la política de participación ciudadana, se ejecutaron y soportaron acorde al resultado esperado, entregable y programación trimestral establecida en el Plan de Sostenibilidad.

6.14. Política de Rendición de Cuentas

Estado actividades	Total
Cumplidas	33
Sin ejecutar	1
En ejecución	0
Sin inicio en primer trimestre	68

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Rendición de Cuentas, Cálculos propios

Respecto a la actividad "Participación en la Rendición de Cuentas de la Administración Distrital", no se observó evidencia que sustenten su ejecución durante el primer trimestre de 2022. Se recomienda adjuntar evidencia(s) de la Audiencia realizada, en la que la SJD haya participado en la Rendición de Cuentas de la Administración Distrital.

En relación con la actividad "planes de mejoramiento, se observó que la actividad se encuentra programada para el cuarto trimestre de la vigencia 2022. Sin embargo, al revisar la página web SJD, numeral 4.9.5 del enlace de transparencia y acceso a la información pública se evidencia publicación de los planes de mejoramiento internos de manera mensual.

6.15. Componente Ambiental

Estado actividades	Total
Cumplidas	6.25
En ejecución	0
Sin inicio en primer trimestre	5.75

Fuente: Plan de Sostenibilidad MIPG 2022 – Componente ambiental, Cálculos propios

Respecto a la actividad "Matriz de aspectos e impactos ambientales, matriz de Riesgos Ambientales actualizada 2022", se evidenció su ejecución durante el primer trimestre de 2022 y su programación durante el segundo trimestre.

En relación con la actividad "Revisiones del componente ambiental realizadas a los procesos de contratación durante la vigencia", se observó programación para el cuarto trimestre y ejecución para el trimestre analizado de 0.25.

No se evidenció programación de la actividad "Evidencias de entregas de bienes y/o residuos de posconsumo para aprovechamiento y/o disposición final", sin embargo, se reportó avance de ejecución durante el primer trimestre de 2022. Se recomienda que se realice la programación en el plan de acuerdo a la periodicidad con la cual se va a ejecutar.

6.16. Política de Seguimiento y Evaluación del Desempeño

Estado actividades	Total
Cumplidas	0
En ejecución	2
Sin inicio en primer trimestre	21

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Seguimiento y Evaluación de Desempeño, Cálculos propios

Para el seguimiento de la presente política, no se aportaron evidencias que dé cuenta de la ejecución del plan de sostenibilidad de MIPG, por lo tanto, esta oficina no pudo realizar verificación de dos (2) actividades programas para el primer trimestre.

6.17. Política de Gestión Documental

Estado actividades	Total
Cumplidas	45
Sin ejecutar	5
En ejecución	0
Sin inicio en primer trimestre	65

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Gestión Documental, Cálculos propios

Respecto a las actividades “Actualizar el Programa Prevención de Emergencias y Atención de Desastres en Archivos”, “Incluir en el procedimiento 2311000-PR-013 comunicación, notificación y/o publicación de actos Administrativos que se debe numerar cada tipo de acto administrativo con un consecutivo único” y “Elaborar un diagnóstico para determinar las necesidades frente a la digitalización de documentos con fines probatorios”, se evidenció que dichas actividades fueron programadas durante el primer trimestre de 2022, sin embargo no se observó evidencia que sustentara la ejecución durante el periodo mencionado.

En relación con la actividad “Incluir actividades de Gestión Documental en POA 2022”, no se aportó evidencia que sustente su ejecución.

Adicionalmente, no se incluyó en el Sistema Integrado de Gestión, el procedimiento para la creación y/o conformación de expedientes electrónicos, actividad que se encontraba programada para el primer trimestre de 2022.

Por otro lado la actividad “Solicitar al Archivo General de la Nación y al Archivo de Bogotá concepto técnico frente a la aplicación de los tiempos de retención en cada fase del ciclo vital de acuerdo a las particularidades de la SJD”, la cual se encontraba programada para ejecutarse durante el primer trimestre de 2022, y en donde en el avance se registró que se está a la espera de una mesa de trabajo con la Dirección Distrital de Archivo de Bogotá, para así proceder a la solicitud del concepto.

6.18. Política de transparencia y acceso a la información y lucha contra la corrupción

Estado actividades	Total
Cumplidas	7
Sin ejecutar	1
En ejecución	0
Sin inicio en primer trimestre	41

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Transparencia y acceso a la información y lucha contra la corrupción, Cálculos propios

Respecto a la actividad Plan de gestión del conocimiento y la innovación 2022 formulado, no se aportó la evidencia que dé cuenta de la ejecución de la actividad mencionada.

Se evidenció programación de actividades en donde en la columna resultado esperado se describe que “no se generan actividades adicionales”, tal como se observa a continuación:

ACTIVIDADES – RESULTADO ESPERADO	NOMBRE DEL RESPONSABLE	MAGNITUD ENTREGABLE	PROGRAMACIÓN TRIMESTRAL				AVANCE FÍSICO
			1er trimestre	2do trimestre	3er trimestre	4to trimestre	
No se generan actividades adicionales	Dirección de Gestión Corporativa - Proceso Gestión Documental	Acta y publicación	2	0	0	0	No aplica
No se generan actividades adicionales	Dirección de Gestión Corporativa - Proceso Gestión Documental	Acta y publicación	2	0	0	0	No aplica

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Transparencia y acceso a la información pública.

Por lo anterior, si no son actividades adicionales, pero son recurrentes y como se reportó en el seguimiento “No aplica”, se sugiere actualizar de manera que tanto la actividad – resultado esperado, sea coherente con la programación y seguimiento. Y en caso de no aplicar, evaluar la pertinencia de retirarlas de la programación.

6.19. Política de Gestión de la información estadística.

Estado actividades	Total
Cumplidas	0
En ejecución	0
Sin inicio en primer trimestre	31

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Gestión de la información estadística, Cálculos propios

Para el seguimiento de la presente política, no se aportaron evidencias que dé cuenta de la ejecución del plan de sostenibilidad de MIPG, por lo tanto, esta oficina no pudo realizar verificación de las trece (13) actividades que iniciaron en el primer trimestre y se encuentran programadas para desarrollar durante el transcurso del año 2022.

6.20. Política de gestión del conocimiento y la innovación.

Estado actividades	Total
Cumplidas	1
En ejecución	0

Sin inicio en primer trimestre	49

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Gestión del conocimiento y la innovación, Cálculos propios

Para el seguimiento de la presente política, no se aportaron evidencias que dé cuenta de la ejecución del plan de sostenibilidad de MIPG, por lo tanto, esta oficina no pudo realizar verificación de las actividades programadas para el primer trimestre, las cuales se relacionan a continuación:

- Formular el Plan de Gestión del Conocimiento y la Innovación correspondiente a la vigencia 2022
- Identificar, capturar, clasificar y organizar el conocimiento explícito contenido en los Sistemas de Información de la entidad
- Contar con un inventario del conocimiento explícito de la entidad actualizado, de fácil acceso y articulado con la política de gestión documental.
- Identificar, clasificar, priorizar y gestionar el conocimiento relevante para el logro de la misionalidad de la entidad.
- Contar con el personal que evalúe, implemente, haga seguimiento y lleve a cabo acciones de mejora al Plan de Acción de Gestión del Conocimiento y la Innovación, en el marco del MIPG.
- Emplear, divulgar, documentar y evaluar métodos de creación e ideación para generar soluciones efectivas a problemas cotidianos de la entidad
- Contar con espacios de ideación e innovación
- Evaluar los resultados de los procesos de ideación adelantados en la entidad y analiza los resultados.
- Desarrollar pruebas de experimentación, documentar y analizar los resultados
- Implementar una estrategia de cultura organizacional orientada a la gestión del conocimiento y la innovación en la entidad y analizar sus resultados.
- Identificar, analizar, evaluar y poner en marcha métodos para aplicar procesos de innovación en la entidad.
- Identificar, clasificar y actualizar el conocimiento tácito de la entidad para la planeación del conocimiento requerido por la entidad.
- Desarrollar análisis descriptivos, predictivos y prospectivos de los resultados de su gestión para determinar el grado avance de las políticas a cargo de la entidad y toma acciones de mejora.
- Contar con estrategias y planes de comunicación para compartir y difundir el conocimiento que produce la entidad tanto al interior como al exterior de esta, a través de herramientas físicas y digitales.
- Desarrollar proyectos de aprendizaje en equipo (PAE) y jornadas del conocimiento dentro de su planeación anual de acuerdo con las necesidades de conocimiento de la entidad. Evaluar los resultados para llevar a cabo acciones de mejora.

De acuerdo con lo anterior, se recomienda aportar las evidencias que den cuenta de las actividades programadas, con el fin de tener herramientas para lograr medir el avance del plan de sostenibilidad de esta política.

Es importante tener en cuenta, que todas las actividades programadas deben evaluarse, con el fin de que la toma de decisiones este fundamentada en las evidencias que demuestran la ejecución de cada actividad.

6.21. Política de Control Interno.

Estado actividades	Total
Cumplidas	0
En ejecución	0
Sin inicio en primer trimestre	9

Fuente: Plan de Sostenibilidad MIPG 2022 – Política de Control Interno, Cálculos propios

Se evidenció que la política en el Plan de Sostenibilidad de MIPG, no tiene actividades programadas para el primer trimestre de 2022.

7. RECOMENDACIONES

En cumplimiento del rol de enfoque hacia la prevención, definido en el artículo 16 del Decreto 648 de 2017 y teniendo en cuenta la información descrita en el presente informe, la Oficina de Control Interno se permite efectuar, de la manera más atenta, las siguientes recomendaciones:

- Se recomienda iniciar la ejecución de las actividades que, si bien no se han vencido, tenían fechas de inicio en el primer trimestre y no reportan avances. Así mismo, adjuntar las evidencias que den cuenta de aquellas actividades que registraron avance en su ejecución, pero no se encuentran sustentadas con los respectivos soportes.

- Se recomienda cuantificar la totalidad de las actividades establecidas en el aparte relacionado con programación trimestral y que sea consistente con lo registrado en la columna magnitud entregable y en el resultado esperado.

- En la política de conflicto de intereses se sugiere registrar la actividad relacionada con el diligenciamiento del reporte de declaración de bienes y rentas y conflicto de intereses por parte de los contratistas de la SJD.

- Se sugiere que en el Plan de Sostenibilidad de MIPG, se describan actividades que efectivamente se van a ejecutar en la vigencia 2022.

- Revisar la pertinencia de modificar la periodicidad de algunas de las actividades programadas, con el fin que sean acordes a la gestión realizada por la Entidad.

- En el momento de definir el avance de las actividades programadas, se recomienda que se realice una verificación entre las evidencias suministradas, las metas establecidas en las actividades del Plan de Sostenibilidad de MIPG y la descripción del avance reportado en la matriz de seguimiento, con el fin de que las tres fuentes de información mencionadas sean consistentes entre sí.

- Se recomienda revisar y atender las principales observaciones que en el presente informe se realizaron específicamente sobre algunas actividades asociadas a cada política del plan de sostenibilidad de MIPG.

- Respecto a la política de gobierno Digital, se recomienda analizar la pertinencia de formular actividades, resultado de los análisis correspondientes, teniendo en cuenta que en la columna “actividades resultado esperado”, no son actividades sino comentarios relacionados con el ítem del autodiagnóstico. Es importante que se realice la actualización del plan asociado a la política teniendo en cuenta las recomendaciones y análisis presentado en el cuerpo del presente informe.

- En el anexo Nro. 1 Informe de Seguimiento Modelo de Seguridad y Privacidad de la Información de la Secretaria Jurídica Distrital, la Oficina de Control Interno detalla las principales conclusiones y recomendaciones observadas, para lo cual se sugiere la revisión y análisis de la pertinencia de incorporarlas en los planes de acción de la vigencia.

- Se sugiere realizar revisión a la calidad de la información reportada por los responsables del plan, en cuanto a organización, redacción y ortografía. Así mismo publicar en la página web la elaboración del plan y los seguimientos trimestrales, para su divulgación y consulta.

(Original Firmado)
CAROLINA LOZANO ARDILA
Jefe Oficina de Control Interno (E)

Proyectó: Carolina Lozano Ardila – Profesional Especializado.
Zulma Yanet Gómez Perales – Contratista
Martha Liliana Barrera Diaz – Profesional Universitario
Revisó / Aprobó: Olga Milena Corzo Estepa – Jefe Oficina de Control Interno.

Anexos:
Anexo 1 Informe de Seguimiento Modelo de Seguridad y Privacidad de la Información de la Secretaria Jurídica Distrital

1. Objetivo

Realizar seguimiento a las actividades ejecutadas que sustentan el avance en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Secretaría Jurídica Distrital, respecto al ciclo PHVA y los controles administrativos establecidos en el formato Instrumento de Evaluación MSPI DAFP, evaluando su nivel de cumplimiento.

2. Alcance

Realizar seguimiento al avance en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Secretaría Jurídica Distrital, con fecha de corte 25 de abril de 2022, respecto al diagnóstico, planificación, implementación, evaluación de desempeño y mejora continua establecidos en el ciclo PHVA y la implementación de los controles administrativos definidos en el Anexo A del estándar ISO/IEC 27001:2013 y en el formato Instrumento de Evaluación MSPI DAFP.

3. Criterios

- Anexo 1 Modelo de Seguridad y Privacidad MSPI, Ministerio de Tecnologías y las comunicaciones, febrero 2021.
- Circular 33 de 2017 expedida Alta Consejería Distrital de Tecnologías de Información y comunicaciones.
- Artículo 2.2.17.5.6 del Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Anexo A Norma ISO 27001:2013. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información. Requisitos.
- Documento metodológico ámbito 6. Valoración de la madurez de la seguridad. Alta consejería de la TICS, diciembre de 2018,
- Construcción y Actualización de Normograma, código 2310100-PR-085
- Guía para el Registro y la Clasificación de Activos de Información, código 2310200-GS-001
- Acuerdo de Niveles de Servicios ANS, código 2310200-GS-003
- Guía Tratamiento de Riesgos de Seguridad de la Información, código 2310200-GS-009
- Guía para el Registro del Índice de Información Clasificada y Reservada, código 2310200-GS-012
- Guía de Seguridad y Privacidad de la Información Seguridad Digital y Continuidad de la Operación de los servicios TIC, código 2310200-GS-013
- Manual de la Política de Tratamiento y Protección de Datos Personales, código 2310200-MA-014
- Manual de Gestión de Incidentes de Seguridad de la Información, código 2310200-MA-015
- Registro de Activos de Información e Índice de Información Clasificada y Reservada, Código 2310200-PR-025
- Plan de Contingencia, código 2310200-PL-003

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

- Vinculación de Servidores Públicos en Cargos de Libre Nombramiento y Remoción, código 2311300-PR-069
- Desvinculación de Servidores Públicos, código 2311300-PR-074
- Vinculación en Periodo de Prueba, código 2311300-PR-114
- Teletrabajo, código 2311300-PR-117
- Vinculación de Servidores Públicos en Provisionalidad, código 2311300-PR-118
- Estudios Previos Contratación Directa, código 2311600-PR-050
- Control Disciplinario Ordinario, código 2310430-PR-029
- Control Disciplinario Verbal, código 2310430-PR-030
- Segunda Instancia de Procesos Disciplinarios, código 2310430-PR-079
- Segunda instancia, código 2310430-PR-123
- Primera instancia etapa juzgamiento verbal, código 2310430-PR-124
- Primera instancia etapa juzgamiento ordinario, código 2310430-PR-125
- Primera instancia etapa instrucción, código 2310430-PR-126
- Instrumento de evaluación del MSPI de la SJD a 25 de abril de 2022[1]

4. Metodología

- Revisión del formato Instrumento de Evaluación MSPI de la Secretaría Jurídica Distrital, con fecha de corte 25 de abril de 2022.
- Revisión documental de los manuales, guías y procedimientos mencionados en el numeral 3 del presente informe.
- Verificación de la información consignada en la página web de la Secretaría Jurídica Distrital, tales como Manual de la Política de tratamiento y protección de datos personales, Guía de Seguridad y Privacidad de la Información Seguridad Digital y Continuidad de la Operación de los servicios TIC, Guía para el registro y clasificación de activos de información, Registro de Activos de Información 2021 y Guía para el Registro y la Clasificación de Activos de Información.
- Entrevista realizada al Oficial de Seguridad de la Información, los días 8 y 13 junio de 2022.

5. Diagnóstico del Modelo de Seguridad y Privacidad de la Información.

"*El diagnóstico permite a los sujetos obligados establecer el estado actual de la implementación de la seguridad y privacidad de la información para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación".*[2]

[1] Herramienta elaborada para identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información". Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre sin fines lucrativos, por esta razón se prohíbe la comercialización y explotación de la misma. (https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/)

[2] Anexo 1 Modelo de Seguridad y Privacidad MSPI, Ministerio de Tecnologías y las comunicaciones, febrero 2021, página 20

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Seguimiento: El diagnóstico se realizó mediante la aplicación del instrumento de Evaluación MSPI, con fecha de corte 31 de diciembre de 2019, el cual presentó un nivel de avance del PHVA de 32% y una evaluación de la efectividad de los controles de administrativos como se detalla a continuación:

Evaluación de la Efectividad de los Controles Administrativos

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación diciembre 2019	Calificación Objetivo	Efectividad de controles
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	**GESTIONADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	45	100	**EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	72	100	**GESTIONADO**
A.8	GESTIÓN DE ACTIVOS	49	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	20	100	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14	100	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	100	**INICIAL**
A.18	CUMPLIMIENTO	35	100	**REPETIBLE**

Fuente: Instrumento de Evaluación MSPI SJD, diciembre 2019

Ciclo PHVA

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Diciembre 2019 Entidad	% Avance Esperado
2015	Planificación	30%	40%
2016	Implementación	2%	20%
2017	Evaluación de desempeño	0%	20%
2018	Mejora continua	0%	20%
TOTAL		**32%**	**100%**

Fuente: Instrumento de Evaluación MSPI SJD, diciembre 2019

6. Controles Administrativos del MSPI a abril de 2022.

"Estos controles están orientados a los temas de seguridad de la información que no están directamente relacionadas con las áreas tecnológicas de la entidad, y contemplan entre otras cosas la evaluación, implementación, revisión y mejoras de la Política de Seguridad de la Información, la evaluación de la definición de las responsabilidades para la gestión de la seguridad de la información y si están acordes con las necesidades de la entidad, la evaluación en la entidad de la seguridad de la información, la revisión y evaluación de los acuerdos de confidencialidad, la evaluación de la cooperación con autoridades y grupos de interés y la revisión de la documentación y formalización de procedimientos de la entidad. Estas pruebas incluyen los

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

controles dados en el Anexo A de la Norma ISO 27001:2013 de los dominios A5, A6, A7, A8, A17 y A18" [3], y los criterios establecidos en el dominio A15.

Teniendo en cuenta la última medición realizada por la Oficina de TICS (corte 25 de abril), se procede a continuación a presentar los resultados del seguimiento a los controles que hacen parte de cada uno de los dominios definidos en el instrumento:

6.1. A5 Políticas de seguridad de la información

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Abril 2022	Calificación Objetivo	Evaluación de efectividad de control
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**

Fuente: Instrumento de Evaluación MSPI SJD, abril 2022

Análisis de los Subrequisitos

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.5	**Políticas de seguridad de la información**			
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	Lineamiento: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	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 partes externas pertinentes.	Se evidenció que la política de Seguridad de la Información se encuentra definida en la Resolución No. 174 de 2021 y Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013.	Se recomienda publicar de forma correcta la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013, así como la publicación de la Resolución 174 de 2021 en la página web de la Entidad.
A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	Al realizar revisión de las actas del Comité de Gestión y Desempeño Institucional de la vigencia 2021, se observó que mediante acta No. 6 de fecha 10 de agosto, se realizó aprobación de la Política de seguridad de la información y del plan estratégico de seguridad de la	Para la revisión de la política de Seguridad de la Información, se recomienda tener en cuenta lo establecido en el Artículo 6 de la Resolución 174 de 2021 que refiere que dicha revisión se realice de manera anual o antes si existiesen modificaciones que así lo

[3] Documento metodológico ámbito 6. Valoración de la madurez de la seguridad. Alta consejería de la TICS, diciembre de 2018, página 17

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			información. Adicionalmente mediante acta No. 9 de 8 de noviembre de 2021, se realizó actualización de la política de protección de datos personales (numeral 3).	requieran, antes del 7 de septiembre de 2022. Se recomienda que para dicha revisión se presente a la Alta Dirección: avances desde que se aprobó la política, posibles rezagos y mejoras a implementar.

6.2. A6 Organización de la seguridad de la información

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Abril 2022	Calificación Objetivo	Evaluación de efectividad de control
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**

Fuente: Instrumento de Evaluación MSPI SJD, abril 2022

Análisis de los Sub-requisitos

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.6	**Organización de la seguridad de la información**			
A.6.1	Organización interna	Lineamiento: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Los roles y responsabilidades en Seguridad de la Información se encuentran definidos en el numeral 4.2.11 de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, en donde se especifican los del Secretario Jurídico Distrital, Nivel Directivo, Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, Comité Operativo y mesas de trabajo técnico de Seguridad de la información, Gestores de Activos, Propietario del Activo, Custodio del Activo y Contratistas, proveedores y terceros. Se debe tener en cuenta que el Comité Operativo y mesas de trabajo técnico de Seguridad de la Información sesiona en el marco de los Subcomités de Autocontrol, definidos en la Resolución 078 de 2018. Dicho comité se encuentra conformado por	Se recomienda que, dentro de los roles y responsabilidades de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se incluya lo pertinente con el Comité de Gestión y Desempeño Institucional y que se encuentre alineado con el numeral 5 del artículo 1 de la Resolución 097 de 2020. Así mismo incluir lo relacionado con la gestión de incidentes en SI. Se recomienda que en la guía mencionada anteriormente se defina quien es el responsable de la protección de los activos de información.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			funcionarios y contratistas de la Oficina de Tecnología de la Información y las Comunicaciones. Se encuentra identificado el responsable del MSPI (Jefe de la Oficina de Tecnología de la Información y las Comunicaciones), los propietarios del activo y para la gestión del riesgo de SI (Jefe OTICS). . Adicionalmente, la resolución 097 de 2020 "Por la cual se modifica el artículo 3 de la Resolución 054 de 2018 "Por el cual se crea el Comité Institucional de Gestión y Desempeño de la Secretaría Jurídica Distrital" y se toman otras determinaciones", en el numeral 5 del artículo 1 se argumenta: " Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información". Por último se evidenció que los roles y responsabilidades para la detección de incidentes se encuentran especificados en el numeral 4 Roles perfiles y responsabilidades del Manual de Gestión de Incidentes de Seguridad de la Información, código 2310200-MA-015, en donde se argumenta que la Oficina de Tecnología de Información y las Comunicaciones es el responsable de "Detectar Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información".	
A.6.1.2	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	Se encuentran definidos los niveles de autorización, en la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, en el numeral 4.5.1.1, Política de control de acceso, en donde se argumenta que Todas las áreas junto con la Oficina de Tecnologías de la Información y las Comunicaciones asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización.	Se sugiere que en el numeral analizado, se especifique los niveles de autorización definidos en la SJD, y la periodicidad de verificación realizada por parte de la Oficina de Tecnología de la Información y las comunicaciones.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
		activos de la organización.		
A.6.1.3	Contacto con las autoridades	Control: Se deben mantener los contactos apropiados con las autoridades pertinentes.	En el numeral 7 de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se tiene definido el contacto con las autoridades en temas de Seguridad de la información. En dicha guía se argumenta "La Secretaría Jurídica Distrital debe mantener contacto con todas las entidades que representan autoridad en temas de seguridad de la información con el fin de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, se mantendrán contactos con las siguientes entidades especializadas en temas relativos a la seguridad de la información: MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones, FIRST – Forum of Incident Response and Security Teams, COLCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia, CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia, CCP – Centro Cibernético Policial y SIC: Superintendencia de Industria y Comercio Se evidenció que el contratista asesor de seguridad de la información se encuentra incluido dentro del grupo WhatsApp "seguridad digital DC" liderado por la Alta Consejería Distrital TIC. Adicionalmente, se observó incidente de seguridad informática el 26 de abril de 2022, el cual fue reportado a Csirtgob del Ministerio del Tecnología de la Información y las Comunicaciones y de la Alcaldía de Bogotá. El reporte se relacionó con un ataque cibernético en el servidor donde está instalado el componente IDM en el ambiente de pruebas de LegalBog. Se detectó por la lentitud y cambios en los roles, perfiles y permisos dentro de la carpeta de configuración de este servicio. El ataque fue contenido a través de la instalación y configuración de un nuevo servidor de IDM en ambiente de pruebas de LegalBog, se	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			deshabilitó la salida a internet de todos los servidores que hacen parte del ambiente de pruebas de LegalBog, bloqueó en el firewall algunas direcciones IP originadas desde Indonesia, instalación de antivirus autorizado de la entidad en el servidor IDM en los ambientes de pruebas y preproducción.	
A.6.1.4	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Se evidenció que el contratista asesor de seguridad de la información se encuentra incluido dentro del grupo WhatsApp "seguridad digital DC" liderado por la Alta Consejería Distrital TIC. De igual forma asiste a capacitaciones, sensibilizaciones sobre seguridad de la información y gestión de riesgos con el Min Tics, Alta Consejería Distrital y Secretaría General.	
A.6.1.5	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.	En el numeral 4.2.1.2. Seguridad de la Información en Gestión de Proyectos de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se establece que: "La Oficina de Tecnologías de Información y las Comunicaciones desarrollará e incorporará en el desarrollo de sus proyectos en la parte concerniente a los riesgos asociados al proyecto, incluirá una identificación y evaluación de riesgos de seguridad de la información, para los cuales se deben definir controles de seguridad que aporten a su mitigación". Por otro lado, se observó que la Oficina de Tecnologías de la Información y las Comunicaciones creo el documento Guía de	Teniendo en cuenta que en Matriz de riesgos del Proyecto LegalBog, se evidenció que se estableció un nuevo Plan de Mitigación para veintiséis (26) de los treinta y un (31) riesgos identificados en el monitoreo reportado el 10 de mayo de 2021 en el cual se discriminan responsables y actividades de seguimiento, no se evidenció un nuevo monitoreo que dé cuenta del seguimiento realizado a dichos planes de mitigación. Por lo cual se recomienda dejar constancia de los seguimientos correspondientes, a partir del último monitoreo reflejado en el documento mencionado.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			gestión de riesgos proyectos de TI, código 2310200-GS-018, el 18 de marzo de 2022. Adicionalmente, se evidenció la elaboración de la matriz de riesgos del proyecto LegalBog, que, de acuerdo con el último monitoreo realizado en el mes de mayo de 2021, cuenta con treinta y un (31) riesgos identificados.	
A.6.2	Dispositivos móviles y teletrabajo	Lineamiento: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
A.6.2.1	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.	La política para dispositivos móviles se encuentra establecida en el numeral 4.2.2.1 de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, la cual argumenta: La Secretaría Jurídica Distrital, controla, gestiona y aprueba el manejo de los dispositivos móviles (teléfonos inteligentes, portátiles, discos duros, USB, DVD) institucionales que hagan uso de los sistemas de información y/o equipos de la entidad. La Oficina de Tecnologías de la Información y las Comunicaciones debe establecer las configuraciones aceptables para los dispositivos institucionales o personales que hagan uso de los servicios provistos por la Secretaría Jurídica distrital. Los usuarios de los dispositivos móviles institucionales deben evitar el uso de estos en lugares que no les ofrezcan garantías de seguridad física para evitar pérdida o hurto. Los usuarios de los dispositivos móviles institucionales no deben modificar las configuraciones de seguridad, ni desinstalar software o instalar programas en los dispositivos móviles institucionales bajo su responsabilidad. Al conectar un dispositivo móvil a la red de la SJD, el propietario del dispositivo acepta las políticas definidas en el presente manual. Respecto a los requisitos de protección física, se observó que se encuentran documentados en el numeral 4.7.2.1 de guía mencionada, el cual da lineamientos protección física y eléctrica a la infraestructura tecnológica de la Entidad, pero no especifica las directrices	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			relacionadas con la protección de dispositivos móviles. Así mismo se evidenció que la política de seguridad de la información (código 2310200-GS-013) contempla las restricciones para la instalación de software (numeral 4.8.5.1.), los requisitos para las versiones de software de dispositivos móviles y para aplicar parches (numeral 4.10.2.4.), restricción de la conexión a servicios de información (numeral 4.5.4.1.), restricción de Acceso a Información, protección contra software malicioso (numeral 4.8.2) y Copias de Respaldo (Backup) (numeral 4.8.3.). No obstante, lo anterior, no se evidenció la definición de lineamientos para el uso de servicios y aplicaciones web.	
A.6.2.2	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.	La política de teletrabajo se encuentra establecida en el numeral 4.2.2.2 de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, la cual argumenta: La Oficina de Tecnologías de la Información y las Comunicaciones designará personal con el fin de que realice la inspección técnica a los puestos de trabajo con el fin de garantizar que la comunicación y operación de los equipos de cómputo sea eficiente. Con relación a la información, dado que esta se considera como el recurso intangible de mayor importancia, es necesario que a fin de prevenir cualquier anomalía se establezcan servicios de antivirus, respaldo o backup, acceso seguro a través de VPN (Virtual Private Network - Red Privada Virtual) y acceso restringido a aplicaciones. Por otro lado, la definición de las políticas de seguridad debe garantizar: Confidencialidad: asegurar el acceso a la información únicamente por las personas autorizadas, que son los teletrabajadores; Integridad: mantener los datos libres de modificaciones no autorizadas; Disponibilidad: garantizar que la información esté en disposición para los teletrabajadores en cualquier momento, de tal forma que puedan desarrollar sus actividades y Autenticación: identificar al usuario	Se sugiere relacionar dentro de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, los formatos relacionados con teletrabajo y en los cuales se relaciona aspectos de seguridad de la información. Se recomienda mantener el listado autorizaciones de VPN actualizadas, de acuerdo con los funcionarios y contratistas de la Entidad.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			generador de la información. De igual forma como se debe propender por reducir las amenazas relacionadas con los recursos intangibles, también se deben establecer los procedimientos relacionados con la protección de los recursos tangibles a través de un análisis de riesgos ocasionados por la implementación de teletrabajo, como por ejemplo establecer procesos de manejo de equipos, pólizas de seguros, mantenimiento de equipos, entre otros. En la política se incluye la seguridad Física, los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización. Adicionalmente tiene en cuenta la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo (numeral 4.7.2.6). La revisión del licenciamiento de software se realiza en el formato Visitas DomiciliariaTeletrabajo.2311300-FT-261. Dicho formato contiene las características específicas requeridas de hardware, software, conectividad y antivirus necesarios para el desarrollo de las funciones de manera remota. Las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el tele trabajador está autorizado a acceder; así como la revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen, se encuentran incluidos en los formatos 2311300-FT-269 Acuerdo de Voluntariedad de Teletrabajo, 2311300-FT-261 Visita Domiciliaria Teletrabajo y 2311300-FT-220 Evaluación por el Jefe Inmediato Teletrabajo y 2311300-PR-117 Teletrabajo En el numeral 4.5.2.4. en la Guía código 2310200-GS-013 se encuentra definida la cancelación de los derechos de usuario se en donde se argumenta que: La Dirección de Gestión Corporativa y los supervisores de los	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			contratistas son los responsables de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo a la Oficina de Tecnologías de la Información y las Comunicaciones. Cuando se solicite una cuenta institucional se debe justificar e informar de la persona responsable de dicho buzón. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella, la Oficina de Tecnologías de la Información y las Comunicaciones podrá eliminar dicha cuenta. Por otro lado al revisar la base de la asignación de VPN remitida por la oficina de Tics se evidenció que se encuentran incluidos tres (3) funcionarios que en la actualidad no tiene relación laboral vigente con la Entidad. (Vicky Chacón, Nancy Aldana y Vanessa Salas.	

6.3. A7 Seguridad de los recursos humanos

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Abril 2022	Calificación Objetivo	Evaluación de efectividad de control
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	93	100	**OPTIMIZADO**

Fuente: Instrumento de Evaluación MSPI SJD, abril 2022

Análisis de los Subrequisitos

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.7	**Seguridad de los recursos humanos**			
Núm.	**Nombre**	**Descripción / Justificación**		
A.7.1	Antes de asumir el empleo	Lineamiento: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos	En el numeral 4.3.1. Selección de personal de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se argumenta que: dentro de los procesos de contratación de personal o prestación de servicios se deberá realizar la verificación de antecedentes cuando así lo amerite y en los casos que se considere necesario, se	Se recomienda que en los procedimientos Vinculación de Servidores Públicos en Cargos de Libre Nombramiento y Remoción, Vinculación en Periodo de Prueba y Vinculación de Servidores Públicos en Provisionalidad, se incluya

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
		y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	realizará el estudio de seguridad del personal que va a ingresar a laborar en la entidad. La Dirección de Gestión Corporativa es el área encargada de realizar la verificación de los antecedentes, de estudios, de experiencia, de referencia laborales y revisar que estén acordes con los estudios previos de acuerdo con las políticas de contratación que existan en la Secretaría. La Dirección de Gestión Corporativa debe garantizar que los funcionarios de la Secretaría firmen un Acuerdo y/o Cláusula de Confidencialidad; este documento debe ser anexado a los demás documentos relacionados con la ocupación del cargo. La verificación de antecedentes del personal de planta, se encuentran definidos en las siguientes actividades de procedimientos. - 2311300-PR-069 Vinculación de Servidores Públicos en Cargos de Libre Nombramiento y Remoción; Actividades 4 Elaborar Formato de Certificación de Cumplimiento de Requisitos, 5 Validar la hoja de Vida del candidato en el SIDEAP y actividad 17 Elaborar Firmar y Acta de Posesión (en donde se encuentra la verificación de los antecedentes la información de las consultas en la Procuraduría, Antecedentes Judiciales de la Policía,). En esta la última actividad no se encuentra relacionada la verificación de antecedentes fiscales de Contraloría, Disciplinarios de Personería y Medidas Correctivas. - 2311300-PR-114 Vinculación en Periodo de Prueba; actividades 8 Elaborar Formato de Certificación de Cumplimiento de Requisitos, 17 Validar la hoja de Vida del candidato en el SIDEAP y 20 Se elabora el acta de posesión con la información del candidato, la información del cargo y la información de las consultas en la Procuraduría, Antecedentes Judiciales de la Policía. - 2311300-PR-118 Vinculación de Servidores Públicos en Provisionalidad; actividades 3 Evaluar si el candidato al empleo cumple con los requisitos mínimos exigidos en la normatividad, 4 Elaborar Formato de Certificación de Cumplimiento de Requisitos, 5 Validar la hoja de Vida del candidato en el SIDEAP y 15 Elaborar y Firmar Acta de Posesión Elaborar el acta de posesión con la información del candidato, la información del cargo y la información de las consultas en la Procuraduría, Antecedentes Judiciales de la Policía, para firma del candidato y el Secretario Jurídico Distrital y/o el	lo relacionado con la verificación de los antecedentes fiscales de Contraloría, Disciplinarios de Personería y Medidas Correctivas. Se sugiere relacionar dentro de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, los procedimientos relacionados con la vinculación de servidores públicos y los relacionados con la selección de contratistas. Por otro lado, se recomienda implementar un control con el fin de realizar verificación de la suscripción del acuerdo de confidencialidad de la información por parte de todos los funcionarios o contratistas de la SJD.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			Director de Gestión Corporativa. Para la verificación de los antecedentes del personal contratista se tienen implementados los siguientes mecanismos: - Se diligencia 2311600-FT-083 Lista de Verificación y Control de Documentos para contratación V8, en donde se encuentra los antecedentes fiscales disciplinarios y de policía. - Procedimiento 2311600-PR-050 Estudios Previos Contratación Directa, actividades 21 Solicitar documentación que acredite el cumplimiento de los requisitos y 22 Verificar la idoneidad y experiencia del futuro contratista según corresponda. Para los casos de vinculación de funcionarios o suscripción de contrato, se solicita el diligenciamiento del formato 2310200-FT-268 Acuerdo de Confidencialidad de la Información, antes de la formalización de la posesión o contrato.	
A.7.1.2	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.	Los acuerdos relacionados con la SI se establecen con la suscripción del formato 2310200-FT-268 Acuerdo de Confidencialidad de la Información. Para el caso de los funcionarios de planta. la verificación de la suscripción de este formato se encuentra incluida en el formato 2311300-FT-095 Requisitos para tomar posesión del cargo. Para el caso de vinculación mediante la modalidad de contrato de prestación de servicios, no se observó mecanismos de verificación de la suscripción.	Se recomienda incluir el formato 2310200-FT-268 Acuerdo de Confidencialidad de la Información, dentro de la lista de verificación y control de documentos para contratación, código 2311600-FT-083, con el fin de verificar la suscripción por parte del personal contratista.
A.7.2	Durante la ejecución del empleo	Lineamiento: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	En numeral 4.3.2.1. Responsabilidad de la Dirección, de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se argumenta: Garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá extenderse al personal de contratistas o terceros, cuando sus responsabilidades así lo exijan. Para que el personal se encuentre informado en	Se recomienda socializar en la entidad el uso de los canales de denuncia interna para el reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información ("denuncias internas").

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			aspectos relacionados con Seguridad de la Información se observó que durante el 2022, se ha realizado la publicación de cinco (5) piezas comunicacionales sobre TIPS para la información personal y corporativa (boletín interno de comunicaciones de febrero 7,8, 10, 11 y 15) y tres (3) piezas comunicacionales relacionadas con las Características de una contraseña robusta (boletín interno de comunicaciones los días 14, 15, 17 de marzo). Por otro lado, no se evidenció que se cuente con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información ("denuncias internas"). Esta actividad se realiza a través del proceso de control interno disciplinario.	
A.7.2.2	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, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	De acuerdo con memorando 3-2022-1559 de fecha 17 de febrero de 2022, la Oficina de Tecnologías de la Información y las Comunicaciones remitió al Despacho de la SJD, las necesidades de comunicación para la presente vigencia. De acuerdo con esto, se observó once (11) temas a comunicar, las cuales se encuentran relacionadas con la seguridad de la información. A la fecha del presente seguimiento, se han realizado: - La publicación de cinco (5) piezas comunicacionales sobre TIPS para la información personal y corporativa (boletín interno de comunicaciones de febrero 7,8, 10, 11 y 15 de 2022) - Tres (3) piezas comunicacionales relacionadas con las Características de una contraseña robusta (boletín interno de comunicaciones los días 14, 15, 17 de marzo de 2022). De acuerdo a entrevista realizada al contratista Asesor de Seguridad de la Información, se argumentó que durante la vigencia 2022, no se han realizado charlas relacionadas con la toma de conciencia en seguridad de la información, se tiene programadas para el segundo semestre. Se evidenció que, durante el 2021, se realizó charla sobre temas de seguridad con asistencia de veintitrés (23) personas. Por otro lado, no se observó que en el Plan Institucional de Capacitación de la vigencia 2022 (Resolución 010) se haya incluido temas relacionados con seguridad de la información o	Se recomienda la elaboración del plan de comunicación, sensibilización y capacitación en materia de seguridad de la información, debidamente revisado y aprobado por la Alta Dirección, que incluya prácticas como: campañas, folletos y boletines, actualización y socialización a nuevos funcionarios y contratistas, periodicidad de la actualización de los planes de toma de conciencia, entre otros asociados en el instrumento de evaluación del MSPI.. Se recomienda ejecutar las actividades programadas referente a las charlas relacionadas con la toma de conciencia en seguridad de la información y la aplicación de la herramienta para medir el nivel de apropiación y conocimiento en temas de Seguridad de la Información.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			tratamiento de datos personales. Respecto a la encuesta en la Secretaría Jurídica Distrital con el fin de medir el nivel de apropiación y conocimiento en temas de Seguridad de la Información, en entrevista se informó que dicha encuesta se tiene programada para realizar en diciembre de 2022.	Las evidencias que sustentan las charlas en seguridad de la información cuenten con fecha, hora y tema tratado. Por último, incluir temas relacionados con seguridad y privacidad de la información en el Plan Institucional de Capacitación de la secretaria Jurídica Distrital.
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	En el numeral 4.3.2.3 Proceso Disciplinario de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se argumenta que: En caso de que un servidor, proveedores, o partes interesadas incumplan estas políticas por negligencia o intencionalmente, la Entidad se reserva el derecho de tomar las medidas correspondientes, tales como acciones disciplinarias, suspensión, despido, acciones legales, reclamo de compensación por daños u otros. En el caso de que un funcionario se vea involucrado en incumplimiento de estas políticas se aplicará lo establecido en el Código Disciplinario Único. La Dirección Distrital de Asuntos Disciplinarios será la encargada de investigar y de ser necesario iniciar el proceso disciplinario. Desde el proceso de control interno disciplinario se tienen definidos los siguientes procedimientos: 2310430-PR-029 Control Disciplinario Ordinario, 2310430-PR-030 Control Disciplinario Verbal, 2310430-PR-079 Segunda Instancia de Procesos Disciplinarios, 2310430-PR-123 Segunda instancia, 2310430-PR-124 Primera instancia etapa juzgamiento verbal, 2310430-PR-125 Primera instancia etapa juzgamiento ordinario, 2310430-PR-126 Primera instancia etapa instrucción	Se sugiere relacionar dentro de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, los procedimientos aplicables de procesos disciplinarios, en el caso de incumplimientos de directrices relacionadas con seguridad de la información.
A.7.3	Terminación o cambio de empleo	Lineamiento: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que	En la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se tiene establecida la política de desvinculación, licencias,	Se recomienda revisar la viabilidad de suscribir acuerdos de confidencialidad de la información, en el momento

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
		permanecen validos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deberían hacer cumplir.	vacaciones o cambio de labores de los funcionarios y personal provisto por terceros (numeral 4.3.3.3.), en donde se argumenta que la Dirección de Gestión Corporativa debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la entidad llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin. Cada Supervisor de Contrato, director y jefe de Oficina debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a la Dirección de Gestión Corporativa. Esta dependencia debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a la Oficina de Tecnologías de la Información y las Comunicaciones. Para el caso de los contratistas será el supervisor quien informe a la Oficina de Tecnologías de la Información y las Comunicaciones, lo que corresponda en cada caso particular. Adicionalmente, y mediante Procedimiento 2311300-PR-074 Desvinculación de Servidores Públicos, en la actividad 7 "Recibir documentación asociada a la entrega del cargo", se encuentra incluido la entrega del formato Constancia de devolución de bienes y cancelación de servicios código 2311500-FT-200. En dicho formato se certifica por parte del jefe de la Oficina de TICS la realización del back up del equipo asignado y desahibilitación de los servicios informáticos. Dicho formato también es utilizado para el personal contratista en el momento de la finalización del contrato. Por otro lado, en la cláusula cuarta del formato 2310200-FT-268 Compromiso de Confidencialidad de Información, se establece la vigencia del compromiso, argumentando: "El presente Compromiso entrará en vigor en el momento de la firma de este, extendiéndose su vigencia hasta un plazo de 2 años después de finalizada la relación entre las partes o, en su caso, la prestación del servicio.".	de presentarse situaciones administrativas tales como encargos, traslados, comisiones, entre otros. Lo anterior dado que el nivel de información que se maneja en algunos cargos es de alta confidencialidad, a lo cual se tiene acceso en las situaciones administrativas anteriormente mencionados. Adicionalmente, el formato 2310200-FT-268, se limita al área, dependencia y acto administrativo cuando se suscribe dicho acuerdo.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

6.4. A8 Gestión de activos

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Abril 2022	Calificación Objetivo	Evaluación de efectividad de control
A.8	GESTIÓN DE ACTIVOS	87	100	**OPTIMIZADO**

Fuente: Instrumento de Evaluación MSPI SJD, abril 2022

Análisis de los subrequisitos

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.8	**Gestión de activos**			
A.8.1	Responsabilidad por los activos	Lineamiento: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	Dentro del Módulo de SGSI del aplicativo SMART, se encuentra el reporte de Activos de información, el cual cuenta con la identificación 285 activos. Por otro lado, en página web se encuentra publicado el inventario de activos en el enlace https://secretariajuridica.gov.co/transparencia/7_datos_abiertos?field_datos_abiertos_target_id=118&field_fecha_de_emision_document_value=All el cual cuenta con 286 registros. Al realizar cotejo de dichas bases se observó diferencia de la identificación de un (1) activo de información de la oficina de TICS el cual corresponde a DISCOS EXTERNOS. Se observó que la última actualización de los inventarios de activos de información fue en septiembre de 2021.	Se recomienda que el inventario de activos de información sea consistente en los diferentes aplicativos de la SJD. (SMART y página Web).
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	La propiedad de los activos de información se encuentra definida en el procedimiento 2310200-PR-025 Registro de Activos de Información e Índice de Información Clasificada y Reservada, ya que de acuerdo a la actividad 1 se establece que los responsables del proceso o dependencia realizan revisión y actualización del Registro de activos de información e índice de Información clasificada y reservada. Adicionalmente, la revisión periódica del inventario y la clasificación de los activos se describe en el numeral 9 de la guía para el registro de activos de información código 2310200-GS-001, ya que en su contenido se relaciona que la actualización, la clasificación, valoración y argumentación legal de la información clasificada y reservada de los activos, se debe realizar cada año o cada vez que se presente alguna modificación.	Se recomienda que el inventario de activos de información del aplicativo SMART cuente con la identificación de la totalidad de los propietarios.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			Respecto al manejo apropiado del activo cuando es eliminado o destruido, se observó que en el numeral 6.1.5. Etiquetado de Activos de Información de la guía mencionada anteriormente argumenta que, para la destrucción de la información pública reservada, información pública clasificada e información pública, en medio Digital y Electrónica se debe aplicar el procedimiento de borrado seguro para los casos en que se requiera de lo contrario aplicar las políticas de Backup (retención). En el caso de información física se debe destruir según lo dispuesto por las tablas de retención documental y los métodos de archivística del Archivo General de la Nación. Se observó que la destrucción lógica de la información se hizo con un software Killdisk y se realiza un acta de eliminación o formateo, a lo cual se remitió actas de borrado de treinta y ocho (38) computadores.	
			Por otro lado, al realizar revisión de los propietarios establecidos en los 285 activos incluidos en el inventario del aplicativo SMART, se evidenció que seis (6) activos no especifican cuál es su "propietario". (actas de medición en conflicto de competencias de entidades, Actas/Actas del Subcomité de Autocontrol, Formato de control de correspondencia, Informes de gestión trimestrales del proyecto 7501, informes de gestión trimestrales del proyecto 7621, memorandos de respuesta), que de acuerdo con la columna denominada dependencia corresponde a la Subsecretaría Jurídica Distrital. Sin embargo, en el registro de activos de información 2021 publicado en la página web, se observó la identificación del propietario de todos los activos de información identificados. Adicionalmente, se evidenció la clasificación de los 285 activos registrados en el inventario consignado en el aplicativo SMART de la siguiente manera: Doscientos treinta y seis (236) como Información pública, treinta y cinco (35) como Información pública clasificada y catorce (14) como Información pública reservada.	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.8.1.3	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.	Se tiene establecido En el numeral 4.4.1.3 Política de Uso Aceptable de los Activos de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, en donde se argumenta que los usuarios, son responsables de un adecuado y racional uso de los activos de información que se usan en los procesos de la Secretaría Jurídica Distrital, es decir, no se pueden usar para propósitos diferentes para los cuales fueron definidos o para temas personales. Los datos de acceso son un elemento personal e intransferible, los usuarios asumen la responsabilidad sobre el buen o mal uso que se dé sobre los sistemas de información de la entidad. La información de la entidad debe ser respaldada de forma frecuente y de acuerdo a las políticas de backups definidas y su almacenamiento debe estar en un lugar apropiado y adecuado, en los cuales se garantice que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes presentados.	
A.8.1.4	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.	El numeral 4.4.1.4. de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, refiere los lineamientos sobre la devolución de los activos en donde se argumenta que: todo activo de propiedad de la Secretaría Jurídica Distrital, asignado a un funcionario de la entidad o a un tercero, deberá ser entregado al retirarse o por cambio de cargo de los funcionarios o a la finalización del contrato. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), contraseñas de ingreso a los sistemas de información, los dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles. En el formato Constancia de devolución de bienes y cancelación de servicios, código 2311500-FT-200, el Jefe de la Oficina de TICS certifica la realización del back up del equipo asignado y des-habilitación de los servicios informáticos. Dicho formato también es utilizado para el personal contratista en el momento de la finalización del contrato.	
A.8.2	Clasificación de la información	Lineamiento: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.8.2.1	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.	En el numeral 4.4.2. Clasificación de la Información de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013 se establece que La Secretaría Jurídica Distrital debe asegurar que la información es tratada y protegida adecuadamente de acuerdo con el nivel de clasificación otorgado. La información física es clasificada de acuerdo con las tablas de retención documental de la entidad. Por otra parte, en el numeral 6.1.3. Clasificación del Activo de Seguridad de la Información de la guía para el registro de activos de información 2310200-GS-01 se establece que la clasificación de activos de información tiene como objeto asegurar la información, basados en la valoración y otras características como el mapa de procesos, como determinante del valor y la clasificación del activo. Se establece que de acuerdo al nivel de integridad disponibilidad y confidencialidad se determina la clasificación del activo en información pública, información pública clasificada o información pública reservada. En dicho numeral se establece los lineamientos respecto a la valoración de la clasificación de los activos de información. Respecto a la revisión de la clasificación del activo, en el numeral 8 de la guía 2310200-GS-01, se establece que se verifica si el activo debe o no permanecer en el registro de activos, se establece que la clasificación, valoración y argumentación legal de la información clasificada y reservada de los activos, se revisa cada año o cada vez que se presente alguna modificación. En consecuencia, se evidenció la clasificación de los 285 activos registrados en el inventario consignado en el aplicativo SMART de la siguiente manera: Doscientos treinta y seis (236) como Información pública, treinta y cinco (35) como Información pública clasificada y catorce (14) como Información pública reservada.	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.8.2.2	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.	El lineamiento sobre etiquetado de la información se encuentra definido en el numeral 4.4.2.2. Etiquetado y Manejo de la Información de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, en donde se profiere que la: Secretaría Jurídica del Distrito desarrollará e implementará un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado. Esta actividad del etiquetado será a cargo del Oficial de Seguridad de la Información. Por su parte en el numeral 6.1.5. Etiquetado de Activos de Información de la guía para el registro de activos de información 2310200-GS-01 se establece que cada activo debe poseer un etiquetado en donde se identifique el nivel de clasificación asignado. El etiquetado debe ser utilizado para aquella información que se encuentre contenida tanto en medio físico como en medio electrónico, de acuerdo con lo indicado en este numeral, en donde se refleja el esquema de clasificación establecido. En este sentido, en el inventario de activos de la SJD las etiquetas se reconocen en la columna clasificación del activo de información y en la parte inferior de los documentos del SIG.	
A.8.2.3	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.	En el apartado del numeral 6.1.5. Etiquetado de Activos de Información de la guía para el registro de activos de información 2310200-GS-01 se establece que para el manejo, procesamiento, almacenamiento y comunicación de la información de acuerdo a la clasificación establecida por la SJD, su adecuado manejo se realiza de acuerdo a información física, documentos digitales, sistemas de información y correo electrónico. Según entrevista realizada al contratista asesor de seguridad de la información, se argumentó que el seguimiento al etiquetado de la información, se efectúa dos veces al año. En consecuencia, se evidenció seguimiento efectuado mediante correo electrónico de fecha 10 de marzo en donde se solicita a los gestores de las dependencias realizar revisión del etiquetado de la información de los activos adjuntos. Así mismo se evidenció informe de actividades de back up de los meses de enero a marzo de 2022.	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.8.3	Manejo de medios	Lineamiento: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.		
A.8.3.1	Gestión de medios removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	En el numeral 4.4.3.1. Gestión de Medios Removibles de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013 se argumenta que la Oficina de Tecnologías de la Información y las Comunicaciones brinda a los funcionarios dispositivos y unidades de almacenamiento removibles tales como dispositivos personales "USB" los cuales están controlados en cuanto a su acceso y uso como medio de La información clasificada como CLASIFICADA o RESERVADA que se desee o tenga que almacenar en medios removibles, debe cumplir con las disposiciones de seguridad indicadas por la Oficina de Tecnologías de la Información y las Comunicaciones, específicamente aquellas referentes al empleo de técnicas de cifrado. La Oficina de Tecnologías de la Información y las Comunicaciones puede restringir el uso de medios de almacenamiento removibles en los equipos de cómputo que sean propiedad de la Secretaría Jurídica Distrital o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción conducente a evitar la fuga de información de la Secretaría Jurídica Distrital por medio de medios removibles.	
A.8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	A la fecha del presente seguimiento, no se evidencia documentado los procedimientos para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas. En entrevista el contratista asesor de seguridad de la información argumentó que está en proceso de elaboración un procedimiento relacionado con el borrado seguro de la información a través de sistema Kill Disk.	Se recomienda formalizar el procedimiento de borrado seguro de la información a través de sistema Kill Disk.
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	En el numeral 4.4.3.2. Transferencia de Medios de soporte físicos de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013 se argumenta que la información clasificada como CLASIFICADA o RESERVADA que se desee almacenar en medios removibles y estos sean transportados fuera de las instalaciones de la Secretaría Jurídica Distrital, debe cumplir con las disposiciones de seguridad indicadas por la Oficina de Tecnologías de la Información y las	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			Comunicaciones, específicamente aquellas referentes al empleo de técnicas de cifrado.	

6.5. A15 Relación con los proveedores

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Abril 2022	Calificación Objetivo	Evaluación de efectividad de control
A.15	RELACIONES CON LOS PROVEEDORES	100	100	**OPTIMIZADO**

Fuente: Instrumento de Evaluación MSPI SJD, abril 2022

Análisis de los Sub-requisitos

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.15	**Relación con los proveedores**			
A.15.1	Seguridad de la información en las relaciones con los proveedores	Lineamiento: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	En el numeral 4.11. Relación con los proveedores de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, específicamente en los numerales 4.11.1. Política de Seguridad en Relación con los Proveedores se argumenta que La Secretaría Jurídica Distrital debe proteger en términos de seguridad la información accedida por los proveedores. y en el numeral 4.11.2. Tratamiento de Seguridad en los Acuerdos con Terceras Partes refiere que en los Contratos o Acuerdos con terceras partes y que impliquen un intercambio, uso o procesamiento de información de la entidad, se deben establecer Acuerdos de Confidencialidad en el manejo de la información. Estos acuerdos deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio. El contrato o acuerdo debe definir claramente el tipo de información que intercambiarán las partes.	
A.15.2	Gestión de la prestación de servicios con los proveedores	Lineamiento: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	Se evidenció seguimiento realizado al contratista ETB enero - abril de 2022, en donde se verifica la disponibilidad del canal de Internet (obteniendo en resultado de 100%), servicios Gsuite (100%), de servidores de dominio (100%), bases de datos (718,2/720)	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

6.6. A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Abril 2022	Calificación Objetivo	Evaluación de efectividad de control
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	44	100	**EFECTIVO**

Fuente: Instrumento de Evaluación MSPI SJD, abril 2022

Análisis de los Subrequisitos

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**			
A.17.1	Continuidad de seguridad de la información	Lineamiento: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	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.	La SJD cuenta con Plan de contingencia código2310200-PL-003. el cual tiene como objetivo proporcionar a la secretaria Jurídica Distrital un Plan de Contingencia Informático, que contenga los procedimientos e instructivos necesarios para poder continuar con las operaciones, procesos y servicios informáticos críticos, en caso de que se llegara a presentar algún siniestro o contingencia. Así como minimizar el impacto que dichos daños pudieran causar. (numeral 2.1) Los requisitos de seguridad de la información se encuentran establecidos en el acápite controles de acceso del numeral 5.2. Seguridad Lógica, del documento 2310200-PL-003 Plan de Contingencia, el cual define los siguientes estándares de seguridad (requisitos mínimos de seguridad en cualquier sistema: ✓ Identificación y Autentificación ✓ Roles ✓ Transacciones ✓ Limitaciones a los Servicios ✓ Modalidad de Acceso ✓ Ubicación y Horario ✓ Control de Acceso Interno ✓ Control de Acceso Externo ✓ Administración. En este punto es necesario resaltar que los sistemas de información Misionales y Administrativos se accede vía Web, pero las actividades para la creación de roles, privilegios y administración de usuarios se encuentran definidas en los procedimientos y lineamientos en cada dependencia de la entidad. La SJD cuenta con 7 aplicativos de LegalBog (servicios misionales), los cuales son considerados como servicios informáticos críticos.	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.17.1.2	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.	Esto se encuentra definido en el numeral 6.2 del Plan de contingencia código2310200-PL-003 Fase II Recuperación y restauración que tiene como objetivos: Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un evento, activando la puesta en marcha de las políticas y procedimientos para restaurar las aplicaciones y datos y Planificar la reactivación dentro de las 12 horas siguientes de producida una contingencia o un desastre, todo el sistema de procesamiento y sus funciones asociadas, así mismo realizar un permanente mantenimiento y supervisión de los sistemas y aplicaciones.	
A.17.1.3	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.	Con el fin de garantizar la continuidad de la seguridad de la información en la SJD, se han realizado pruebas de funcionalidad de LegalBog. Según informe de segundo ejercicio de plan de contingencia de los sistemas de información LegalBog, se concluyó que ha sido un ejercicio necesario para establecer el cumplimiento de los RTO y RPO definidos en caso tal de presentarse inconvenientes en los componentes de WSO2 Identity Server y API Manager. Los resultados del ejercicio determinan que el área de infraestructura está en capacidad de dejar el sistema operativo en un promedio de 5 horas teniendo en cuentas los incidentes presentados definidos previamente en el alcance del ejercicio. Por otro lado, no se evidenció que en el Plan de contingencia código2310200-PL-003, se incluyan lineamientos relacionados con la verificación, revisión y evaluación de la continuidad de la seguridad de la información a intervalos regulares de 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.	Se recomienda incluir dentro del documento Plan de contingencia código2310200-PL-003, procedimientos relacionados con la verificación, revisión y evaluación de la continuidad de la seguridad de la información con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	Redundancias	Lineamiento: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	De acuerdo con entrevista realizada al contratista asesor de seguridad la información se argumentó que la SJD, no cuenta con arquitecturas redundantes, por un tema de presupuestal.	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

6.7. A18 Cumplimiento

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Abril 2022	Calificación Objetivo	Evaluación de efectividad de control
A.18	CUMPLIMIENTO	100	100	**OPTIMIZADO**

Fuente: Instrumento de Evaluación MSPI SJD, abril 2022

Análisis de los Subrequisitos

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.18	**Cumplimiento**			
Núm.	**Nombre**	**Descripción / Justificación**		
A.18.1	Cumplimiento de requisitos legales y contractuales	Lineamiento: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	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.	Se evidenció que, para la identificación de los requisitos legales, se tienen establecidos los siguientes documentos: El normograma de cada proceso se encuentra incluido en la caracterización en el aplicativo SMART. 2310100-PR-085 Construcción y Actualización de Normograma V2 En la página web se encuentra publicado en transparencia y acceso de la información pública, numeral 2 Normativa de la Entidad	
A.18.1.2	Derechos de propiedad intelectual	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.	En el numeral 4.10.1. Requisitos de Seguridad en la Adquisición de los Sistemas de Información de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se establece que "Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor". Así mismo en el numeral 4.10.2.5. Desarrollo de Software Contratado Externamente de la guía mencionada se expresa que los contratos de desarrollo de software con terceros deberán tener claramente definidos los alcances de las licencias, los derechos de propiedad del código desarrollado y los derechos de propiedad intelectual, junto con los	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			requerimientos contractuales relacionados con la calidad y seguridad del código desarrollado. Adicionalmente, en el numeral 4.10.2.6. Prueba de Seguridad en los Sistemas de Información refiere que se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto. Por otro lado, para realizar control de la instalación de software ilegal, la Oficina de Tecnologías de la Información configura el mínimo de privilegios a los usuarios en donde se puede consultar, pero no se puede instalar. Se cuentan con usuarios específicos que tienen como rol administrador de máquina y de red. En el numeral 4.10.2.4 se especifica las restricciones sobre los paquetes de software en donde los cambios a los paquetes de software son autorizados, supervisados y realizados por funcionarios de la oficina de Tecnologías de la Información y las Comunicaciones de la entidad. Si es necesario que un proveedor o contratista realice los cambios al paquete de Software, estos cambios serán realizados bajo el permiso y supervisión de la misma área, con la finalidad de garantizar la confidencialidad e integridad de la información contenida en los computadores, dispositivos móviles, sistemas de información y procesamiento a los que sea necesario realizarle cambios. Se evidenció listado de trescientas cuatro (304) de software instalado en los equipos de la SJD, con fecha de corte 13 de junio de 2022.	
A.18.1.3	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.	Las tablas de retención documental de las once (11) dependencias de la SJD especifican los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Enlace https://www.secretariajuridica.gov.co/transparencia/instrumentos-gestion-informacion-publica/tablas-retencion-documental	
A.18.1.4	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos	En la página web de la SJD se encuentra publicado el Manual de la Política de Tratamiento y Protección de Datos Personales enlace https://www.secretariajuridica.gov.co/manual-de-la-politica-de-tratamiento-y-proteccion-de-	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
		personales, como se exige en la legislación y la reglamentación pertinentes.	datos-personales. Respecto a los responsables, en el numeral 2 del Manual de la Política de Tratamiento y Protección de Datos Personales se establece el alcance en donde se argumenta la Secretaría Jurídica Distrital, se considera como responsable y/o encargado del tratamiento de los datos personales. Referente al repositorio de los datos personales, en el numeral 6.8.1.4. Prueba de la Autorización del 2310200-MA-014 Manual de la Política de Tratamiento y Protección de Datos Personales, se argumenta que La Secretaría Jurídica Distrital dispondrá de los medios tecnológicos o físicos con que cuenta actualmente, e implementará y adoptará las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos, que permitan demostrar cuándo y cómo se obtuvo la autorización por parte de los titulares. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin. En relación con el consentimiento para tratar los datos personales, en el numeral 6.8.1.3. Modo de Otorgar la Autorización del 2310200-MA-014 Manual de la Política de Tratamiento y Protección de Datos Personales refiere que la autorización del Titular puede darse por escrito, de forma oral o mediante conductas inequívocas de éste, que permitan concluir de forma razonable que otorgó la autorización. La autorización puede constar en un documento físico, electrónico (mensaje de datos, Internet, sitios web), o en cualquier otro formato que permita garantizar su posterior consulta. Asimismo, podrá otorgarse mediante un mecanismo técnico o tecnológico idóneo, que permita manifestar su consentimiento de manera electrónica, para a concluir de manera inequívoca que, de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos. En correspondencia con las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos En el numeral 6,24	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
			Seguridad de los Datos Personales 2310200-MA-014 Manual de la Política de Tratamiento y Protección de Datos Personales refiere que La Secretaría Jurídica Distrital, en estricta aplicación del Principio de Seguridad en el Tratamiento de Datos Personales, proporcionará las medidas técnicas humanas y administrativas que sean necesarias para otorgar seguridad a los registros minimizando el riesgo de su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, fallas técnicas. La obligación y responsabilidad de la Secretaría Jurídica Distrital se limita a disponer de los medios adecuados para este fin.	
A.18.1.5	Reglamentación de controles criptográficos	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Los controles criptográficos se encuentran establecidos en el numeral 4.6.1. de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, en donde se argumenta que La Secretaría Jurídica Distrital debe proteger la confidencialidad, integridad y disponibilidad de la información por medio de técnicas criptográficas apropiadas. La Oficina de Tecnologías de la Información y Comunicaciones debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos. Se debe garantizar que el uso de controles criptográficos no entorpezca aquellos controles de seguridad basados en inspección de contenido, tales como filtrado web, antimalware, antispyware, etc. La Oficina de Tecnologías de la Información y las Comunicaciones deberá validar dicha condición y determinar las mejores condiciones de aplicabilidad de los controles criptográficos.	

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.18.2	Revisiones de seguridad de la información	Lineamiento: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		

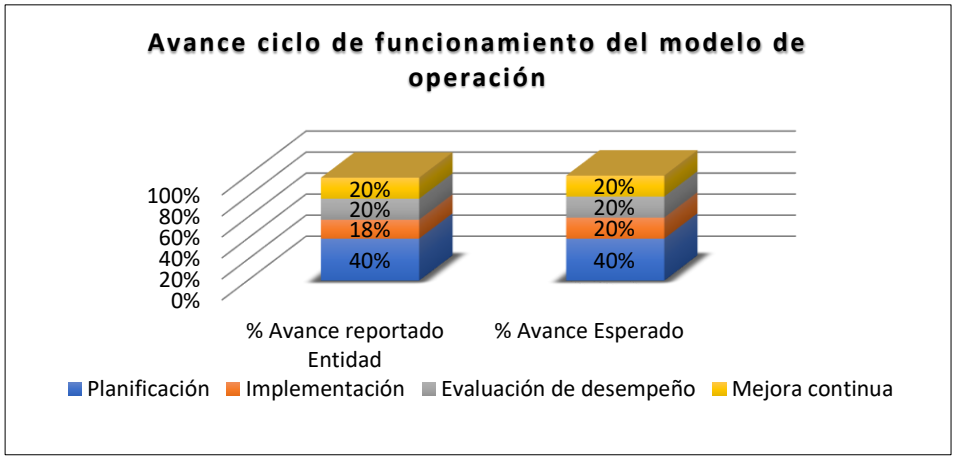
Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI	Recomendación OCI
A.18.2.1	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.	Se evidenció que durante la vigencia 2020, la Oficina de Control interno realizó auditorías al cumplimiento de los requisitos de seguridad de la información establecidos en la política de la SJD, en los Sistemas de Información de apoyo de la entidad SI CAPITAL (PERNO, SAE, SAI), SMART y al sistema Integrado LEGALBOG (en desarrollo). Adicionalmente, el contratista asesor de seguridad de la información en entrevista argumentó que en la actualidad la SJD se encuentra en proceso de revisión del MSPI con apoyo de la Alta Consejería Distrital de las TICS.	
A.18.2.2	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.	La revisión del centro de cómputo se realiza de manera anual a través del mantenimiento de las UPS y cableado. Se realizó mantenimiento preventivo y correctivo durante la vigencia 2021. La revisión de los sistemas de información se realiza cada 3 o 4 meses, en donde se ejecuta depuración de usuarios de información, de las aplicaciones misionales.	
A.18.2.3	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.	La revisión de la seguridad en los sistemas de información se realiza a través del antivirus (revisión de amenazas), WAF (en donde se hace revisiones y genera alertas de posibles ataques en las aplicaciones web) y la utilización del Firewall.	

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

7. Ciclo PHVA

De acuerdo con la información reportada en el instrumento de evaluación del MSPI a 25 de abril de 2022 y el seguimiento realizado por esta oficina, se evidenció que el avance del Modelo de Seguridad y Privacidad de la Información asciende a 98%, el cual por componente se discrimina a continuación:



Fuente: Instrumento de Evaluación MSPI SJD abril 2022, cálculos propios.

A continuación, se detalla el seguimiento cualitativo realizado por cada componente que contiene el ciclo PHVA:

7.1. Planificación

"Para el desarrollo de esta fase se debe utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la Entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI". [4]

[4] Anexo 1 Modelo de Seguridad y Privacidad MSPI, Ministerio de Tecnologías y las comunicaciones, febrero 2021, página 22

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI
Alcance	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	1. El alcance del MSPI se encuentra definido en el numeral 2 de la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013, en el cual se especifica que las políticas serán aplicadas a los procesos estratégicos, misionales y de apoyo de toda la Secretaría Jurídica Distrital. 2. De acuerdo con la verificación documental, se evidenció que el contexto interno y externo se encuentra definido en el numeral 7.2 y las partes interesadas en el numeral 7.3 del Plan Estratégico de Seguridad de la Información PESI, código 2310200-PL-012 y de acuerdo con entrevista realizada al Oficial de Seguridad se argumentó que estos criterios se encuentran alineados con el contexto de la política de calidad de la SJD. Sin embargo, en la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013, no se encuentra, descritos dichos criterios.	1. Respecto al alcance de la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013, se incluya los procesos de control y evaluación. 2. De acuerdo con lo establecido en las "pruebas" definidas en el instrumento de evaluación MSPI, se recomienda incluir dentro del documento Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013, lo relacionado con los aspectos internos y externos que son necesarios para cumplir su propósito, y que afectan su capacidad para lograr los resultados previstos en el SGSI. Así mismo incluir lo relacionado con las partes interesadas del MSPI.
Política de Seguridad y Privacidad de la Información.	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	Se evidenció que la política de Seguridad de la Información se encuentra definida en la Resolución No. 174 de 2021 y Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013. Al revisar el contenido de la guía mencionada, se evidenció que el enlace que se encuentra en el numeral 4.3.1.1 Términos y condiciones laborales, no funciona. Enlace: https://Secretaríajuridica.gov.co/transparencia/atencion-ciudadano/politicas Por otro lado, se observó que en el contenido de la publicación en página web de la guía mencionada, se encuentra el formato de solicitud de publicación en página web Enlace: https://www.Secretaríajuridica.gov.co/transparencia/2_normativa?field_normativa_target_id=165&field_fecha_de_emision_document_value=All Igualmente, no se evidenció publicación de la Resolución 174 de 2021 en la página web de la SJD.	Se recomienda publicar de forma correcta la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operaciones de los Servicios TICS, código 2310200-GS-013, así como la publicación de la Resolución 174 de 2021 en la página web de la Entidad.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI
Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere b. Esté protegida adecuadamente.	El control documental, creación, actualización, eliminación, acceso, uso, preservación, almacenamiento y control de cambios se ve reflejado en el procedimiento Elaboración y Control de Documentos, código 2310100-PR-001, y el Manual Modulo de Documentos del aplicativo SMART.	
Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Los roles y responsabilidades en Seguridad de la Información se encuentran definidos en el numeral 4.2.11 de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, en donde se especifican los del Secretario Jurídico Distrital, Nivel Directivo, Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, Comité Operativo y mesas de trabajo técnico de Seguridad de la información, Gestores de Activos, Propietario del Activo, Custodio del Activo y Contratistas, proveedores y terceros. Se debe tener en cuenta que el Comité Operativo y mesas de trabajo técnico de Seguridad de la Información sesiona en el marco de los Subcomités de Autocontrol, definidos en la Resolución 078 de 2018. Dicho comité se encuentra conformado por funcionarios y contratistas de la Oficina de Tecnología de la Información y las Comunicaciones. Se encuentra identificado el responsable del MSPI (Jefe de la Oficina de Tecnología de la Información y las Comunicaciones), los propietarios del activo y para la gestión del riesgo de SI (Jefe OTICS). Adicionalmente, la resolución 097 de 2020 "Por la cual se modifica el artículo 3 de la Resolución 054 de 2018 "Por el cual se crea el Comité Institucional de Gestión y Desempeño de la Secretaría Jurídica Distrital" y se toman otras determinaciones", en el numeral 5 del artículo 1 se argumenta: " Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información".	Se recomienda que, dentro de los roles y responsabilidades de la Guía de implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, código 2310200-GS-013, se incluya lo pertinente con el Comité de Gestión y Desempeño Institucional y que se encuentre alineado con el numeral 5 del artículo 1 de la Resolución 097 de 2020. Así mismo incluir lo relacionado con la gestión de incidentes en SI. Se recomienda que en la guía mencionada anteriormente se defina el rol de responsables de activos de información y las actividades ejecutar.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI
		Por último se evidenció que los roles y responsabilidades para la detección de incidentes se encuentran especificados en el numeral 4 Roles perfiles y responsabilidades del Manual de Gestión de Incidentes de Seguridad de la Información, código 2310200-MA-015, en donde se argumenta que la Oficina de Tecnología de Información y las Comunicaciones es el responsable de "Detectar Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información".	
Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Dentro del Módulo de SGSI del aplicativo SMART, se encuentra el reporte de Activos de información, el cual cuenta con la identificación 285 activos. Por otro lado, en página web se encuentra publicado el inventario de activos en el enlace https://Secretaríajuridica.gov.co/transparencia/7_datos_abiertos?field_datos_abiertos_target_id=118&field_fecha_de_emision_document_value=All el cual cuenta con 286 registros. Al realizar cotejo de dichas bases se observó diferencia de la identificación de un (1) activo de información de la oficina de TICS el cual corresponde a DISCOS EXTERNOS. Se observó que la última actualización de los inventarios de activos de información fue en septiembre de 2021.	Se recomienda que el inventario de activos de información sea consistente en los diferentes aplicativos de la SJD. (SMART y página Web).
Identificación, análisis y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	Para la presente vigencia se tienen identificados tres (3) riesgos asociados a la Seguridad de la Información los cuales se relacionan a continuación: - Posibilidad de afectación reputacional, por pérdida de la integridad de la información de la entidad y/o la ciudadanía, debido a ejecución de cambios no controlados. (Se acepta el riesgo) - Posibilidad de afectación reputacional, por pérdida de la disponibilidad de la información de la entidad y/o la ciudadanía, debido al vencimiento de licencias, certificados digitales, dominios y/o el uso no autorizado de software o forma de almacenamiento. (Se acepta el riesgo) - Posibilidad de afectación reputacional, por pérdida de la confidencialidad de la información de la entidad y/o la ciudadanía, debido al intercambio de información confidencial sin utilizar mecanismos seguros o cifrado vulnerables. (Se acepta el riesgo) A la fecha del presente seguimiento, los riesgos	En cuanto a la Guía para el Tratamiento de Riesgos de Seguridad de la Información, código 2310200-GS-009, se recomienda revisar su pertinencia toda vez que la Metodología Integrada para la Gestión de Riesgos de la SJD. código 2310100-OT-002 se encuentra alineada a la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del DAFP, la cual ya contiene la metodología de identificación, análisis y valoración de riesgos de seguridad de la información. Respecto a la matriz de riesgos relacionados con seguridad y privacidad de la información, se recomienda que la valoración de estos sea consistente entre las fuentes consultadas.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI
		anteriormente mencionados no se han materializado. Para la identificación, análisis y valoración de los riesgos mencionados anteriormente, se tuvo en cuenta lo definido en la Metodología Integrada para la Gestión de Riesgos de la SJD. código 2310100-OT-002. Sin embargo, se evidenció documento denominado Guía para el tratamiento de riesgos de seguridad de la información, código 2310200-GS-009, en el cual se observó el procedimiento a llevar respecto a la gestión del riesgo de seguridad de la información (análisis del riesgo, riesgo inherente, riesgo residual y escalas de valoración). Por lo anterior se observó que se tienen formalizadas dos metodologías para la gestión de riesgos de seguridad de la información. Al realizar cotejo de los riesgos descritos en la Matriz de riesgos del aplicativo SMART (Muy baja 20%) y los publicados en la página web institucional (Baja 40%) se evidenció, diferencias en la cuantificación de la probabilidad del riesgo "Posibilidad de afectación reputacional, por pérdida de la disponibilidad de la información de la entidad y/o la ciudadanía ,debido al vencimiento de licencias, certificados digitales, dominios y/o el uso no autorizado de software o forma de almacenamiento" , lo cual trae como consecuencia que en el aplicativo SMART el riesgo inherente se ubique en una zona de riesgo baja, mientras que en la página web se ubica como zona de riesgo moderada.	Adicionalmente, se recomienda tener en cuenta la criticidad del activo descrito en el inventario de activos de información, para la identificación análisis y valoración de riesgos de seguridad de la información.
Tratamiento de riesgos de seguridad de la información	Los riesgos deben ser tratados para mitigarlos y llevarlos a niveles tolerables por la Entidad	En la página web de la Secretaría Jurídica Distrital, se tiene publicado como Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la vigencia 2022, La Guía Tratamiento de riesgos de seguridad de la información 2310200-GS-009, enlace https://Secretaríajuridica.gov.co/sites/default/files/2022-01/2310200-GS-009%20Gu%C3%ADa%20Tratamiento%20de%20Riesgos%20de%20Seguridad%20de%20la%20Informaci%C3%B3n_copia_controlada.pdf la cual se publicó el 31 de enero de 2022, en cumplimiento de lo establecido en el artículo 1 del Decreto 612 de 2018. Sin embargo, al revisar su contenido no se evidenció que el plan de tratamiento de riesgos contenga, fechas y responsables con el objetivo de realizar trazabilidad, tal como lo argumenta el numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información de la Guía Anexo 1 modelo de Seguridad	Se recomienda establecer un Plan de tratamiento de riesgos de manera anual que contenga fechas y responsables con el objetivo de realizar trazabilidad. Así mismo dentro del Plan de tratamiento tener en cuenta la Metodología Integrada para la Gestión de Riesgos de la SJD. código 2310100-OT-002, la cual se basa en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del DAFP.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Número requisito	Nombre del control	Descripción del control	Seguimiento OCI
		y Privacidad de la Información del Ministerio de Tecnologías y las Comunicaciones, febrero 2021.	
Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, 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 pertinentes para su cargo.	De acuerdo con memorando 3-2022-1559 de fecha 17 de febrero de 2022, la Oficina de Tecnologías de la Información y las Comunicaciones remitió al Despacho de la SJD, las necesidades de comunicación para la presente vigencia. De acuerdo con esto, se observó once (11) temas a comunicar, las cuales se encuentran relacionadas con la seguridad de la información. A la fecha del presente seguimiento, se han realizado: - La publicación de cinco (5) piezas comunicacionales sobre TIPS para la información personal y corporativa (boletín interno de comunicaciones de febrero 7,8, 10, 11 y 15 de 2022) - Tres (3) piezas comunicacionales relacionadas con las Características de una contraseña robusta (boletín interno de comunicaciones los días 14, 15, 17 de marzo de 2022). De acuerdo con entrevista realizada al contratista Asesor de Seguridad de la Información, se argumentó que durante la vigencia 2022, no se han realizado charlas relacionadas con la toma de conciencia en seguridad de la información, se tiene programadas para el segundo semestre. Se evidenció que, durante el 2021, se realizó charla sobre temas de seguridad con asistencia de veintitrés (23) personas. Por otro lado, no se observó que en el Plan Institucional de Capacitación de la vigencia 2022 (Resolución 010) se haya incluido temas relacionados con seguridad de la información o tratamiento de datos personales. Respecto a la encuesta en la Secretaría Jurídica Distrital con el fin de medir el nivel de apropiación y conocimiento en temas de Seguridad de la Información, en entrevista se informó que dicha encuesta se tiene programada para realizar en diciembre de 2022.	Se recomienda la elaboración del plan de comunicación, sensibilización y capacitación en materia de seguridad de la información, debidamente revisado y aprobado por la Alta Dirección, que incluya prácticas como: campañas, folletos y boletines, actualización y socialización a nuevos funcionarios y contratistas, periodicidad de la actualización de los planes de toma de conciencia, entre otros asociados en el instrumento de evaluación del MSPI.. Se recomienda ejecutar las actividades programadas referente a las charlas relacionadas con la toma de conciencia en seguridad de la información y la aplicación de la herramienta para medir el nivel de apropiación y conocimiento en temas de Seguridad de la Información. Las evidencias que sustentan las charlas en seguridad de la información cuenten con fecha, hora y tema tratado. Por último, incluir temas relacionados con seguridad y privacidad de la información en el Plan Institucional de Capacitación de la secretaria Jurídica Distrital.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

7.2. Implementación

"Una vez culminada las actividades del MSPI de la fase de 7.3 Planificación, se llevará acabo la implementación de los controles, con el fin de dar cumplimiento con los requisitos del MSPI".[5]

Requisito	Descripción	Seguimiento OCI	Recomendación OCI
Planificación y control operacional	Estrategia que se debe ejecutar con las actividades para lograr la implementación y puesta en marcha del MSPI de la entidad.	Se evidenció que se elaboró el Plan Estratégico de Seguridad de la Información, código 2310200-PL-012, el cual tiene como objetivo "Definir una estrategia de Seguridad de la información, en adelante PESI, liderada por el área de Tecnologías de Información y Comunicación - TIC, a partir de la vigencia 2020-2023 que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información". Por otro lado, se evidenció, que mediante acta de reunión de fecha 24 de noviembre de 2021, se realizó seguimiento al cumplimiento del PESI durante las vigencias 2020 y 2021, de acuerdo con los proyectos priorizados en el numeral 9.1 del plan mencionado. Sin embargo, en dicho seguimiento no se evidenció la trazabilidad realizada al Proyecto P.04 "sistema de control de acceso para dispositivos móviles".	Se recomienda que dentro del seguimiento semestral programado al PESI por parte de la Oficina de TICS, se incluyan todos los proyectos priorizados en el numeral 9.1 del plan mencionado.
Implementación de controles	Grado de implementación de controles del Anexo A de la ISO 27001	De acuerdo al instrumento de evaluación del MSPI con fecha de corte 25 de abril de 2022, se evidenció una evaluación de efectividad de controles de 86%, en donde los controles A.7 Seguridad de los recursos humano (93), A8 Gestión de activos (87), A.9 Control de acceso (86), A.11 Seguridad física y del entorno (65), A.12 Seguridad de las operaciones (83), A.13 Seguridad de las comunicaciones (72), A.14 Adquisición, desarrollo y mantenimiento de sistemas (80) y A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio (44) , presentaron una calificación menor a la objetivo la cual en todos los casos asciende a 100.	Se recomienda continuar con la implementación del Modelo de Seguridad y Privacidad de la Información en la SJD:
Implementación del plan de tratamiento de riesgos	Porcentaje de avance en la ejecución de los planes de tratamiento	Se evidenció que los tres (3) riesgos relacionados con seguridad de la información no tienen planes de tratamiento, ya que su nivel de riesgo residual se tipificó como bajo y su tratamiento es aceptar el riesgo. Lo anterior de acuerdo con el literal d del numeral 7 de la metodología Integrada para la Gestión de Riesgos en la Secretaría Jurídica distrital, la cual argumenta "Asumir el riesgo indica que el proceso correspondiente no requiere formular e implementar acciones de tratamiento".	
Indicadores de gestión del MSPI	Indicadores de gestión del MSPI definidos	Con relación con la seguridad de la información, se observó la estructuración de tres (3) indicadores: - Nivel de cumplimiento de implementación del MSPI, el cual tiene como objetivo medir la implementación del modelo de seguridad y privacidad de la información de manera que se cumpla con los criterios de confidencialidad, integridad y disponibilidad y presenta un resultado a abril de 2022 de 100% de las actividades programadas en el trimestre.	

[5] Anexo 1 Modelo de Seguridad y Privacidad MSPI, Ministerio de Tecnologías y las comunicaciones, febrero 2021, página 32

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Requisito	Descripción	Seguimiento OCI	Recomendación OCI
		- Porcentaje de incidentes gestionados relacionados en el marco de la seguridad y privacidad de la información institucional, el cual tiene como objetivo determinar la eficacia en el tratamiento de eventos relacionados con la seguridad de la información, respecto de los eventos reportados por los usuarios o determinadas en las auditorías planeadas para el sistema y resultado a abril de 2022 de 117,65%. (medición trimestral). - Porcentaje de controles de seguridad de la información implementados, el cual tiene como objetivo determinar el grado de avance en la implementación y monitoreo de controles de seguridad de la información (este indicador se medirá a partir del cuarto trimestre de 2021) y resultado a marzo de 2022 de 100% (medición trimestral)	

7.3. Evaluación de Desempeño

"Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG"[6]

Requisito	Descripción	Seguimiento OCI	Recomendación OCI
Plan de seguimiento, evaluación y análisis del MSPI	Plan para evaluar el desempeño y eficacia del MSPI a través de instrumentos que permita determinar la efectividad de la implantación del MSPI.	La evaluación y seguimiento del desempeño y eficacia del MSPI se realizó a través del instrumento de evaluación del DAFP el cual a 25 de abril de 2022, presentó una efectividad de controles de 86%, en donde los controles A.7 Seguridad de los recursos humano (93), A8 Gestión de activos (87), A.9 Control de acceso (86), A.11 Seguridad física y del entorno (65), A.12 Seguridad de las operaciones (83), A.13 Seguridad de las comunicaciones (72), A.14 Adquisición, desarrollo y mantenimiento de sistemas (80) y A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio (44) , presentaron una calificación menor al objetivo, el cual en todos los casos asciende a 100. Se evidenció un avance del ciclo PHVA de 98%.	Se recomienda continuar con la implementación del Modelo de Seguridad y Privacidad de la Información en la SJD:
Auditoría Interna	Plan de auditoría interna	Se evidenció que durante la vigencia 2020, la Oficina de Control interno realizó auditorías al cumplimiento de los requisitos de seguridad de la información establecidos en la política de la SJD, en los Sistemas de Información de apoyo de la entidad SI CAPITAL (PERNO, SAE, SAI), SMART y al sistema Integrado LEGALBOG (en desarrollo). Adicionalmente, el Oficial de Seguridad en entrevista, argumentó que en la actualidad la SJD se encuentra en proceso de revisión del MSPI con apoyo de la Alta Consejería Distrital de las TICS.	

[6] Anexo 1 Modelo de Seguridad y Privacidad MSPI, Ministerio de Tecnologías y las comunicaciones, febrero 2021, página 34

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Requisito	Descripción	Seguimiento OCI	Recomendación OCI
Evaluación del plan de tratamiento de riesgos	Evaluación y seguimiento a los compromisos establecidos para ejecutar el plan de tratamiento de riesgos.	Se evidenció que los tres (3) riesgos relacionados con seguridad de la información (1. Posibilidad de afectación reputacional, por pérdida de la disponibilidad de la información de la entidad y/o la ciudadanía ,debido al vencimiento de licencias, certificados digitales, dominios y/o el uso no autorizado de software o forma de almacenamiento, 2. Posibilidad de afectación reputacional, por pérdida de la integridad de la información de la entidad y/o la ciudadanía, debido a ejecución de cambios no controlados y 3. Posibilidad de afectación reputacional, por pérdida de la confidencialidad de la información de la entidad y/o la ciudadanía, debido al intercambio de información confidencial sin utilizar mecanismos seguros o cifrado vulnerables) no tienen planes de tratamiento, ya que su nivel de riesgo residual se tipificó como bajo y su tratamiento es aceptar el riesgo. Lo anterior de acuerdo con el literal d del numeral 7 de la metodología Integrada para la Gestión de Riesgos en la Secretaría Jurídica distrital, la cual argumenta "Asumir el riesgo indica que el proceso correspondiente no requiere formular e implementar acciones de tratamiento". Adicionalmente, se observó seguimiento a la eficacia de los controles establecidos en los riesgos relacionados con seguridad de la información. De acuerdo con la información consignada en el aplicativo SMART, el ultimo seguimiento fue realizado en el mes de mayo de 2022, a lo cual se evidenció la eficacia de los nueve (9) controles diseñados (tres (3) detectivos y seis (6) preventivos).	
Revisión por la dirección	Los temas de seguridad y privacidad de la información, seguridad digital deben ser tratados y aprobados en el comité institucional de gestión y desempeño,	Al realizar revisión de las actas del Comité de Gestión y Desempeño Institucional de la vigencia 2021, se observó que mediante acta No. 6 de fecha 10 de agosto, se realizó aprobación de la Política de seguridad de la información y del plan estratégico de seguridad de la información. Así mismo mediante acta No. 7 de fecha septiembre 13 de 2021, se realizó revisión por la alta dirección de la eficacia del MSPI (numeral 12) con un avance del 77% y se realizó aprobación de los dos (2) indicadores de seguridad de la información (Porcentaje de incidentes gestionados relacionados en el marco de la seguridad y privacidad de la información institucional y Porcentaje de controles de seguridad de la información implementados). Finalmente, mediante acta No. 9 de 8 de noviembre de 2021, se realizó actualización de la política de protección de datos personales (numeral 3).	

7.4. Mejora Continua

"Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas". [7]

[7] Anexo 1 Modelo de Seguridad y Privacidad MSPI, Ministerio de Tecnologías y las comunicaciones, febrero 2021, página 36

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Requisito	Descripción	Seguimiento OCI	Recomendación OCI
Plan de seguimiento, evaluación y análisis del MSPI	Resultados consolidados del componente evaluación de desempeño	Los resultados consolidados del seguimiento y evaluación del MSPI se observaron en la pestaña "Portada" del instrumento de evaluación del DAFP el cual a 25 de abril de 2022, presentó una efectividad de controles de 86%, en donde los controles A.7 Seguridad de los recursos humano (93), A8 Gestión de activos (87), A.9 Control de acceso (86), A.11 Seguridad física y del entorno (65), A.12 Seguridad de las operaciones (83), A.13 Seguridad de las comunicaciones (72), A.14 Adquisición, desarrollo y manteamiento de sistemas (80) y A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio (44) , presentaron una calificación menor al objetivo, el cual en todos los casos asciende a 100. Se evidenció un avance del ciclo PHVA de 98%.	
Auditoría Interna	Comunicación de los resultados y plan para subsanar los hallazgos y oportunidades de mejora.	Mediante memorando No. 3-2020-7013 del 26/10/2020 y 3-2020-8214 de fecha 01/12/2020 se realizó comunicación por parte de la Oficina de Control Interno a la Oficina de Tecnologías de la Información y las Comunicaciones los informes de auditoría del cumplimiento de los requisitos de seguridad de la información establecidos en la política de la SJD, del sistema Integrado LEGALBOG y de los Sistemas de Información de apoyo de la entidad SI CAPITAL (PERNO, SAE, SAI), SMART respectivamente. Así mismo dichas auditorias se comunicaron al Secretario Jurídico Distrital mediante memorandos No. 3-2020-8813 de fecha 16/12/2020 y 3-2020-7167 de fecha 30/10/2020. Productos de las auditorias mencionadas se realizó suscripción de los siguientes planes de mejoramiento. - Cumplimiento de los requisitos de seguridad de la información establecidos en la política de la SJD, en los Sistemas de Información de apoyo de la entidad SI CAPITAL (PERNO, SAE, SAI), SMART: Planes de mejoramiento No. 468 y 469. A la fecha del presente seguimiento, se observó que el No. 468 se encuentra en estado cerrado - efectivo y el 469 se encuentra cumplido en un 100% y pendiente de la evaluación de la efectividad por parte de esta oficina. - Cumplimiento de los requisitos de seguridad de la información establecidos en la política de la SJD del sistema Integrado LEGALBOG (en desarrollo): se suscribieron los planes de mejoramiento No. 440, 441 y 442, los cuales a la fecha del presente seguimiento se encuentran en estado cerrado - efectivo.	

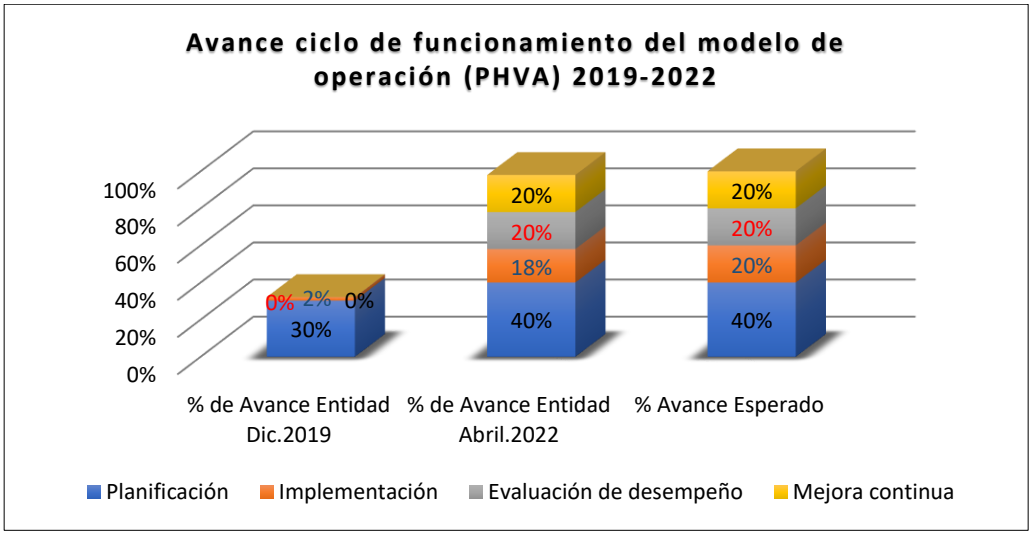
Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Conclusiones y Recomendaciones

Como resultado del seguimiento realizado al Modelo de seguridad y Privacidad de la Información – Controles Administrativos y al Ciclo PHVA del Modelo se pudieron verificar los avances y actividades detalladas en la autoevaluación con corte a abril remitido por la Oficina de TICS, desde la Oficina de Control Interno se han realizado las principales recomendaciones teniendo en cuenta la información verificada.

Respecto a los controles administrativos objeto de análisis del presente seguimiento, se observó que los definidos en A5, A6, A7, A8, A17, A18 y A15, presentaron en su mayoría un avance significativo, teniendo en cuenta el diagnóstico aplicado en diciembre de 2019.

Por otro lado, y teniendo en cuenta los avances del ciclo PHVA por componentes desde la vigencia 2019 a 2022, se evidencia un mayor porcentaje de avance en dos componentes: Evaluación de desempeño y Mejora continua con un incremento del 20% para cada uno. El componente implementación presentó un avance del 16% y el componente de planificación presentó un avance del 10% siendo el menor avance desde la vigencia 2019 a 2022. En términos generales se presentó desde la vigencia 2019 a 2022, un porcentaje de incremento de avance del 66%, pasando del 32% al 98% con el ultimo corte al 25 de abril de 2022.



Fuente: Instrumento de Evaluación MSPI SJD, diciembre 2019 y abril 2022

Lo anterior se refleja en el componente de planeación en la definición de la política, roles y responsabilidades, inventario de activos, procedimientos para el análisis valoración y tratamiento de riesgos, actividades relacionadas con la toma de conciencia, educación y formación en la

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

seguridad de la información. Adicionalmente, en el componente de implementación, la aprobación del PESI y su seguimiento, la implementación de controles establecidos en el MSPI y la definición de indicadores de gestión. En el componente de verificación y mejoramiento, se observó el seguimiento a la ejecución de los controles definidos en la matriz de riesgos relacionados con el Modelo y la revisión por la alta Dirección. Así mismo la realización de auditorías y la ejecución y cumplimiento de planes de mejora.

Se sugiere tener en cuenta las recomendaciones establecidas en los numerales 6 y 7 del presente informe.

(original firmado)
CAROLINA LOZANO ARDILA
Jefe Oficina de Control Interno (E)

Proyectó: Carolina Lozano Ardila – Profesional Especializado.
Martha Liliana Barrera Díaz – Profesional Universitario
Revisó/ Aprobó: Olga Milena Corzo Estepa– Jefe Oficina de Control Interno.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195