FECHA:	25 de julio de 2024	**INFORME PRELIMINAR**	☐	**INFORME DEFINITIVO**	■
PROCESO AUDITADO:	AUDITORÍA AL PROCESO DE GESTIÓN TECNOLÓGICA E INNOVACIÓN, CON ÉNFASIS EN EL ***MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI***				
RESPONSABLE DEL PROCESO:	John Hollman Gómez Corredor – Líder del proceso				
EQUIPO AUDITOR:	Luz Dary Amaya Peña, Contratista OCI Wellfin Jhonathan Canro Rodriguez, Jefe OCI				

RESUMEN EJECUTIVO DE LA AUDITORÍA:

Objetivo:

Verificar el cumplimiento de la entidad en cuanto a la planificación e implementación de los lineamientos definidos por el Ministerio de las Tecnologías de la Información en el Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI, expedido en octubre de 2021; con el fin de emitir recomendaciones que contribuyan a generar acciones para el fortalecimiento del Sistema de Control Interno y el Modelo Integrado de Planeación y Gestión – MIPG de la entidad.

Alcance:

La verificación se realizará con base en la planificación e implementación de los siguientes requerimientos mínimos y obligatorios por parte de la entidad con corte a abril de 2024 y los cuales se encuentran definidos en el Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021:

Diagnostico

1. Herramienta de autodiagnóstico (Análisis GAP), del estado actual de la entidad respecto a la Seguridad y privacidad de la Información.

Fase de Planeación

2. Plan de Seguridad y Privacidad de la Información vigencias 2023 y 2024
3. Los documentos que se deben tener en la fase de planeación que son:
    a. Alcance MSPI
    b. Acto administrativo con las funciones de seguridad y privacidad de la información.
    c. Política de seguridad y privacidad de la información.
    d. Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información
    e. Procedimiento de inventario y Clasificación de la Información e infraestructura crítica
    f. Metodología de inventario y clasificación de la información e infraestructura crítica
    g. Procedimiento de gestión de riesgos de seguridad de la información
    h. Plan de tratamiento de riesgos de seguridad de la información
    i. Declaración de aplicabilidad
    j. Manual de políticas de Seguridad de la Información
    k. Plan de capacitación, sensibilización y comunicación de seguridad de la información
4. Contexto de la entidad
5. Partes interesadas

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

6. Acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.
7. Acto administrativo con la adopción de la Política de seguridad y privacidad de la información
8. Roles y responsabilidades
9. Procedimiento de inventario y clasificación de la información y documento metodológico de inventario y clasificación de la información.
10. Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno
11. Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño y Declaración de aplicabilidad, aceptada y aprobadas en el comité de gestión institucional
12. Incluir dentro de los proyectos de inversión de la entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido
13. Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital y Plan de comunicaciones del modelo de seguridad y privacidad de la información

Fase de Operación

14. Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto y Evidencia de la implementación de los controles de seguridad y privacidad de la información

Fase de Evaluación

15. Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto 612 de 2018 e informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.

Nota de aclaración: La evaluación del numeral 18 incluye la valoración de 114 controles, dicha actividad depende de la declaración de aplicabilidad de la entidad; por lo tanto, el alcance de este ítem podría ser parcial, dependiendo el volumen de la información que surge en el proceso de validación.

Analizada la información, se presenta el consolidado de los aspectos que requieren formulación de plan de mejoramiento dado que incumplen con la normativa vigente:

Tabla No. 1 Consolidado de Hallazgos

TEMA No.	El Hallazgo y su Descripción
1	**Tema: Diagnostico MSPI** Revisado el documento de autodiagnóstico presentado el día 14/05/2024 por el grupo auditado se identificaron las siguientes debilidades: • Se evidencia que el mismo no cumple con los mínimos requeridos tal y cómo se describe en la tabla No.1 donde se observa que campos relevantes como responsable, evidencia y brecha no fueron diligenciados. • Se evidencia que no es posible establecer si este documento es el inicial, lo anterior dado que en el contenido al parecer se evalúan los criterios en la vigencia 2020 (antes de la expedición del MSPI) pero en la fecha de elaboración registra julio de 2023, dato que tampoco es consistente pues en la hoja denominada *Portada*, solo están datos de la vigencia 2020

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

	Esta situación permite concluir que se incumple lo establecido en el No. 6 Diagnostico del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic. **Responsable del plan de mejoramiento:** Oficina de Tecnologías de la Información.
2	**TEMA: Roles y Responsabilidades** Revisado el documento MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN versión 4 del año 2023 se identificaron las siguientes debilidades: • Se evidencia que no se han definido de manera específica los Roles y Responsabilidades del MSPI para el responsable de Seguridad de la Información, el Comité Institucional de Gestión y Desempeño Institucional, la Oficina Asesora Jurídica, la Unidad de Talento Humano y la Oficina de Control Interno. lo anterior denota incumplimiento del numeral 7.2.3 Roles y responsabilidades del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 • Se evidencia que no se ha expedido el acto administrativo de nombramiento de un profesional que dependa de un área estratégica, que no sea la Oficina de Tecnologías de la Información, que deberá ser incluida como miembro del Comité de Gestión institucional con voz y voto y en el Comité de Coordinación Institucional de Control Interno con voz; lo anterior denota incumplimiento del numeral 7.2.3 Roles y responsabilidades del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 **Responsable del plan de mejoramiento:** Oficina de Tecnologías de la Información
3	**TEMA: Identificación de activos de información e infraestructura crítica y Valoración y tratamiento de los riesgos de seguridad de la información** Revisada la información recibida por parte de la Oficina de Tecnologías de la Información el día 20/05/2024 que corresponde al formato de Inventario de Activos de Información de 10 de los 17 procesos que tiene la entidad, y analizada la Política de Administración de Riesgo de la entidad publicada en la página web a la fecha (19/07/2024) y teniendo en cuenta la información recibida en la mesa de trabajo realizada con los profesionales de la Oficina de Tecnologías de la Información el día 21/05/2024, se identificaron las siguientes debilidades: • Se evidencia que para el 41% de los procesos (Gestión de Comunicaciones, Gestión de Recaudo, Control, Inspección y Fiscalización, Gestión Financiera y Contable, Gestión Documental, Control Interno Disciplinario y Protección de Datos Personales), no se cuenta con Inventario de Activos de Información; esto incumple lo establecido en el numeral 7.3.1 Identificación de activos de información

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

	e infraestructura critica del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic. • El inventario del proceso Gestión del Talento Humano solo cuenta con 1 activo de información definido. Situación que no es consistente con las diferentes funciones que ejecuta la unidad y de las cuales se podrían identificar como activos de información tales como nómina, situaciones administrativas del personal de planta, actividades de capacitación y bienestar, temas de seguridad y salud en el trabajo, entre otros. • Se evidencia que la política de administración de riesgos de la entidad no tiene establecidos los lineamientos específicos para la identificación y tratamiento de riesgos de seguridad de la información. • Se evidencia que la entidad no ha aplicado el tratamiento de riesgos de la seguridad de la información Lo anterior incumple los numerales 7.3.1 Identificación de activos de información e infraestructura critica, 7.3.2 Valoración de los riesgos de seguridad de la información y 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic. **Responsable del plan de mejoramiento:** Oficina de Tecnologías de la Información
4	**TEMA: Partes Interesadas del MSPI** Revisado el documento denominado Caracterización de Usuarios y Partes Interesadas, recibido el día 22/05/2024 por parte de la Oficina de Planeación, se evidencia que incumple lo establecido en el numeral 7.1.2. Necesidades y expectativas de los interesados del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic, dado que en el mismo no se identifican expresamente las partes internas y externas que pueden influir directamente en la seguridad y privacidad de la información, así como tampoco se determinan los requisitos legales, reglamentarios y contractuales de dichas partes. **Responsable del plan de mejoramiento:** Oficina de Tecnologías de la Información y Oficina de Planeación
5	**TEMA: Funciones del Comité Institucional de Gestión y Desempeño frente al MSPI** Revisada la información recibida el día 27/05/2024 por parte de la Oficina de Planeación en relación con las resoluciones de creación y modificación de la conformación del Comité Institucional de Gestión y Desempeño, y analizada la resolución vigente No. 107 de 2023 *"Por la cual se integra y se adopta el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Lotería de Bogotá*", se evidencia que en el artículo *5°*

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

	Funciones, no se incorporan las funciones relacionadas con seguridad y privacidad de la información, lo que conlleva al incumplimiento de los numerales 7.2.1 Liderazgo y Compromiso y 7.2.2 Política de seguridad y privacidad de la información del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic. **Responsable del plan de mejoramiento:** Oficina de Planeación
6	**TEMA: Competencia, toma de conciencia y comunicación** Revisada la información recibida el día 4 y 27 de junio de 2024 por la Unidad de Talento Humano y la Subgerencia Comercial y de Operaciones, respectivamente, y analizados los resultados de la encuesta de percepción enviada a todos los colaboradores de la entidad el día 11 de junio de 2024 se evidencian las siguientes debilidades: 1. No se ha involucrado al 100% de los funcionarios de la entidad en la implementación del MSPI, esto se concluye dado que solo 14 trabajadores oficiales diligenciaron la encuesta 2. Falta concientización de los colaboradores en cuanto al MSPI tal y como se evidencia en la Tabla No. No. 4 3. No se ha realizado por parte de la Subgerencia Comercial y de Operaciones la identificación de necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Lo anterior conlleva al incumplimiento del numeral 7.4.2 Competencia, toma de conciencia y comunicación del Documento Marco – Modelo de Seguridad y Privacidad de la Información **Responsable del plan de mejoramiento:** Unidad de Talento Humano, Subgerencia Comercial y de Operaciones y Oficina de Tecnologías de la Información.

Fuente: Elaboración propia.

Para el desarrollo de la auditoría especial al proceso Gestión Tecnológica e Innovación - MSPI, se realizaron en síntesis las siguientes actividades:

- El día 09/05/2024 se remitió el memorando 3-2024-839 adjuntado el documento Aviso de Inicio de Auditoría
- El día 10/05/2024 se realizó la reunión de apertura de la auditoría y se suscribió la carta de representación
- El día 14/05/2024 se realizó la Mesa No. 1 donde se revisaron los temas de autodiagnóstico, plan de Plan de Seguridad y Privacidad de la Información y política de seguridad de la información
- El día 14/05/2024 se realizó el requerimiento No. 1 dirigido a la Oficina de Tecnología y Oficina de Planeación solicitando el documento de autodiagnóstico, plan de Plan de Seguridad y Privacidad de la Información con soportes de la vigencia 2023 y 2024 y el documento de Política de Seguridad de la Información con la respectiva acta de aprobación; el requerimiento fue contestado el 14/105/2024
- El día 16/05/2024 se remitió requerimiento No. 2 a la Oficina de Planeación sobre acto administrativo de adopción del MSPI y acta del Comité Institucional de Gestión y Desempeño; el cual fue respondido el mismo día.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- El día 17/05/2024 se realizó mesa de trabajo No. 2 donde se abordaron los siguientes temas: Roles y Responsabilidades y activos de información
- El día 17/05/2024 se envió requerimientos No. 3 (Oficina de Planeación), 4 y 5 (Oficina TI) relacionados con contexto, partes interesadas, roles y responsabilidades y activos de información, contestados el 22/05/2024
- El día 21/05/2024 se realizó mesa de trabajo No. 3 y se trataron los temas de política y plan de tratamiento de riesgos y declaración de aplicabilidad.
- El día 22/05/2024 se envió el requerimiento No. 6 a la Oficina de Planeación relacionado con liderazgo y recursos asignados al modelo, el cual fue contestado el 27/05/2024
- El día 22/05/2024 se envió el requerimiento No. 7 a la Oficina de Tecnologías de la Información relacionado con la declaración de aplicabilidad, el cual fue contestado el día 23/05/2024.
- El día 27/05/2024 se realizó Mesa de trabajo No. 4 con la Oficina de Tecnologías de la Información donde se socializaron los hallazgos 2,3 y 4 y se trató el tema de declaración de aplicabilidad
- El día 27/05/2024 se envió el requerimiento No. 8 a la Secretaría General, Oficina de Tecnología de la Información y Unidad Financiera, la cual esta relacionada con los recursos asignados por la entidad para la implementación del MSPI, la cual fue contestado el 04/06/2024 informando que la Unidad Financiera no contaba con la información, por lo tanto, se reenvió a la Oficina de Tecnologías de la Información el mismo día; la respuesta definitiva se recibió el 04/07/2024
- El día 30/05/2024 se envió requerimiento No. 9 a la Unidad de Talento Humano, el cual está relacionado con capacitaciones y formación en temas del MSPI, el mismo fue respondido el 04/06/2024
- El día 30/05/2024 se envió requerimiento No. 10 a Comunicaciones el cual está relacionado con la comunicación del MSPI, fue contestado el día 27/06/2024
- El día 04/06/2024 se envió a la Oficina de Tecnologías de la Información el requerimiento No. 11 solicitando agenda para validación de los controles del anexo A, la respuesta fue dada vía telefónica el día 05/06/2024.
- El día 06/06/2024 se realizó Mesa No.1 para verificación de implementación de controles definidos en la declaración de aplicabilidad
- El día 11/06/2024 se realizó Mesa No.2 para verificación de implementación de controles definidos en la declaración de aplicabilidad
- El día 11/06/2024 se elaboró y envió encuesta en FORMS para determinar la percepción de los colaboradores de la Lotería frente al MSPI
- El día 12/06/2024 se realizó Mesa No.3 para verificación de implementación de controles definidos en la declaración de aplicabilidad
- El día 13/06/2024 se realizó Mesa No.4 para verificación de implementación de controles definidos en la declaración de aplicabilidad relacionados con la Unidad de Recursos Físicos y Talento Humano
- El día 26/06/2024 se realizó Mesa No.5 para verificación de implementación de controles definidos en la declaración de aplicabilidad relacionados con directorio activo
- El día 02/07/2024 se realizó el análisis del resultado de la encuesta y se consolidó en el informe preliminar de auditoría
- El día 19/07/2024 se envía informe preliminar con radicado No. 3-2024-1270 del 19/07/2024
- El día 24/07/2024 la Oficina de Tecnología de la Información envía respuesta al informe preliminar con radicado 3-2024-1304, así mismo el mismo día se recibe comunicación verbal por parte de la Oficina de Planeación aceptando los hallazgos a su cargo.
- El día 25/07/2024 se realiza reunión de cierre y se remite informe final de auditoría

Limitación al alcance:

En el alcance de la auditoría se define “Fase de Evaluación 15. Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto 612 de 2018 e informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos”. No obstante, en desarrollo de la presente auditoría se evidencia que la entidad aún no

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

ha llegado a esta fase, tal y como se detalla en el Hallazgo No. 4, por lo anterior este criterio se incluirá en una auditoria posterior cuando la entidad alcance un mayor nivel de madurez en la implementación del MSPI.

Modelo Integrado de Planeación y Gestión – MIPG

El MIPG incluye en el numeral 3.4.2 la Política de Seguridad Digital, la cual propende porque las entidades identifiquen, gestionen, traten y mitiguen los riesgos de seguridad digital. El modelo define que la implementación de la política se hará a través de la adopción del Modelo de Gestión de Riesgos de Seguridad Digital, que es desarrollado y socializado por MinTic.

En la presente auditoría se verificaron los aspectos de la Política de Seguridad Digital, los cuales están incorporados en los lineamientos definidos en el Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI expedido por MinTic.

CONFORMIDADES:

Conformidad No. 1

Tema: Política de Seguridad de la Información y Manual de políticas de Seguridad de la Información

Criterio: Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI

7. Planificación

(…) Los documentos que se deben generar en esta fase son:

Política de seguridad y privacidad de la información
Manual de políticas de Seguridad de la Información

Condición:

El día 14/05/2024 se recibió por correo electrónico enviado por la Oficina de Tecnologías de la Información el documento denominado MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN, el cual fue aprobado en Comité Institucional de Gestión y Desempeño el día 16/08/2023, tal y como consta en el numeral 8 del acta de dicha sesión. En el numeral 5 del documento aprobado se incluye el capítulo 5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

El documento esta publicado en el link:
https://loteriadebogota.com/wp-content/uploads/MANUAL-PSI-16082023-Aprobado-CIGD-04-09-2023.pdf

Se concluye que la entidad cumple el criterio, no obstante, se identifica y formula la observación y Recomendación No. 1, respectivamente.

Conformidad No. 2

Tema: Alcance MSPI

Criterio: Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI

7.1.3 Definición del alcance del MSPI

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Determinando los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la entidad.
Determinando a que procesos y recursos tecnológicos se realizará la implementación del MSPI.

Condición:

El día 14/05/2024 se recibió por correo electrónico enviado por la Oficina de Tecnologías de la Información el documento denominado MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN, el cual fue aprobado en Comité Institucional de Gestión y Desempeño el día 16/08/2023, tal y como consta en el numeral 8 del acta de dicha sesión. En el numeral 2 del documento aprobado se incluye el alcance del sistema, así:

"2. ALCANCE Este documento describe las políticas de seguridad de la información definidas por la LOTERÍA DE BOGOTÁ, teniendo en cuenta la política de Gobierno Digital establecida mediante el Decreto 1008 de 2018, el Modelo de Seguridad y Privacidad de la Información, la ley 1581 de 2012 de protección de datos personales y demás legislación aplicable. Estas políticas se aplican en todo el ámbito de la LOTERÍA DE BOGOTÁ, que incluye los funcionarios, contratistas, entes de control, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la LOTERÍA DE BOGOTÁ, compartan, utilicen, recolecten, procesen, intercambien o consulten su información".

El documento esta publicado en el link:
https://loteriadebogota.com/wp-content/uploads/MANUAL-PSI-16082023-Aprobado-CIGD-04-09-2023.pdf

Se concluye que la entidad cumple el criterio

Conformidad No. 3

Tema: Plan de Seguridad y Privacidad de la Información vigencias 2023 y 2024

Criterio: Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI

7. Planificación

Para el desarrollo de esta fase se deben 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.

Condición:

El día 14/05/2024 se recibió por parte de la Oficina de Planeación el link de acceso a los Planes de Seguridad y Privacidad de la Información de las vigencias 2023 y 2024 y los soportes remitidos por la Oficina de Tecnología de la Información donde reportan los avances con corte a 31 de diciembre de 2023 y a 31 de marzo de 2024.

Así mismo se valida que el plan formulado para la vigencia 2024 está publicado en el link: https://loteriadebogota.com/wp-content/uploads/10.Plan-de-Seguridad-y-Privacidad-de-la-Informacion-2024.pdf

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Se concluye que la entidad ha cumplido en términos generales, no obstante, al revisar el detalle de los soportes de dichos planes se evidencian algunos aspectos que son susceptibles de mejora, por lo tanto se formula la Observación No. 3 del presente informe.

Conformidad No. 4

Tema: Contexto de la organización

Criterio: Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI

7.1.1 Comprensión de la organización y de su contexto

Determinar los elementos externos e internos que son relevantes con las actividades que realiza la entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la entidad.

Condición:

El día 22/05/2024 se recibe por parte de la Oficina de Planeación la matriz de contexto Institucional, la cual permite evidenciar que la entidad realizó en el segundo semestre de la vigencia 2023 la identificación de Debilidades, Amenazas, Fortalezas y Oportunidades en cada uno de los procesos. Adicional a ello se definieron estrategias para los factores con calificación de criticidad igual o mayor a 3. Dichas estrategias tienen como objetivo mitigar la amenaza (control), fortalecer la debilidad (acción de mejora), aprovechar las oportunidades, o mantener las fortalezas.

Por otra parte se revisa Acta del Comité Institucional de Gestión y Desempeño del día 17/11/2023 numeral 3: en la cual se soporta la socialización y aprobación del Contexto Institucional.

Teniendo en cuenta lo anterior se concluye el cumplimiento del criterio. No obstante, se incluye en el presente informe la Observación No. 5 y Recomendaciones 7 y 8.

Conformidad No. 5

Tema: Recursos MSPI

Criterio: Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI

7.4.1 Recursos

La entidad debe determinar y proporcionar los recursos necesarios para adoptar el MSPI, teniendo en cuenta que es un proceso transversal de la entidad, se requiere que se disponga de los recursos financieros, humanos (dedicación de horas/hombre) de sus colaboradores y en general cualquier recurso que permita la adopción, implementación, mantenimiento y mejora continua del MSPI.

Condición:

El día 04/07/2024 se recibe de la Oficina de Tecnologías de la Información el cuadro detallado con los contratos incluidos en el Plan Anual de Adquisiciones 2024 y el estado de cada uno de ellos, del cual se cita a continuación los procesos que ya han sido suscritos en esta vigencia o que eran prorrogas de contratos suscritos en la vigencia 2023:

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Tabla No. 2 Procesos contractuales

Descripción	Valor total estimado	Contrato
Actualizar la infraestructura de red, instalación, implementación y puesta en funcionamiento de los equipos Firewall, switch y Access point con los servicios asociados basadas en las especificaciones técnicas requeridas por la Lotería de Bogotá.	$ 384,180,000.00	OC 119270 de 2023
Adquirir el soporte técnico y mantenimiento para el sistema de información misional, así como el suministro de las páginas web para el control de los sorteos extraordinarios de la Lotería Bogotá	$ 103,536,250.00	22 - 2024
Adquirir la bolsa de créditos y los servicios de soporte técnico y mantenimiento requeridos para garantizar la continuidad de los sistemas de información en la nube Oracle de la Lotería de Bogotá	$ 101,679,832.00	OC 121211 de 2023
Adquirir la suscripción, licenciamiento y soporte técnico de Adobe Illustrator, plugins Wordpress del portal web y software de cametización Easy Card Creator Premium para la Lotería de Bogotá.	$ 12,117,982.00	27 de 2024
Adquirir los servicios de custodia, logística y transporte de medios magnéticos para la Lotería de Bogotá.	$ 9,869,790.00	54 de 2023
Mantenimiento preventivo y correctivo con bolsa de repuestos de aire acondicionado ubicado en el centro de cómputo de la Sede principal	$ 11,059,337.00	102 de 2023
Adquisición de productos y servicios Microsoft para la Lotería de Bogotá a través del Acuerdo de Precios de Colombia Compra Eficiente.	$ 60,960,193.00	OC 118511 de 2023
Canal Dedicado acceso Internet principal	$ 6,609,234.00	OC 107135 de 2023
Prestar los servicios de acceso a Internet mediante un canal dedicado tipo Oro de 256 Mbps y un enlace de conectividad de datos en fibra óptica para conectar la sede principal de la Lotería carrera 32A No. 26-14 con la sede de Venecia AK 54 No.47 A- 08 Sur.	$ 6,230,100.00	OC 117425 de 2023
Prestar el servicio de alojamiento (hosting) y soporte al alojamiento de la página Web de la Lotería de Bogotá conforme a las especificaciones técnicas requeridas, incluyendo el certificado digital de sitio seguro (SSL).	$ 17,206,553.00	89 de 2023
Prestar servicios profesionales para el análisis, desarrollo, implementación y puesta en producción de nuevos requerimientos del portal web de la Lotería de Bogotá, así como el soporte técnico y el mantenimiento de la plataforma web actual.	$ 44,729,700.00	95 de 2023
Prestar servicios profesionales para la formulación, implementación, actualización y acompañamiento a procesos de tecnología relativos al modelo de seguridad y privacidad de la información de la Lotería de Bogotá.	$ 94,920,000.00	36 de 2024
Licencias Antivirus	$ 32,790,000.00	18 de 2024
Contratar los servicios bajo el modelo SAS para mantener el sistema administrativo y financiero de la LOTERÍA DE BOGOTÁ Bolsa de horas para realizar desarrollos adicionales necesarios.	$ 336,088,000.00	06 de 2024

Fuente: Oficina de Tecnologías de la Información

Se puede concluir que la entidad ha destinado recursos para la implementación del MSPI. No obstante, a través del presente informe se evidencia tanto en los hallazgos como en las observaciones y recomendaciones que es importante fortalecer y si es posible incrementar la asignación de dichos recursos.

Por otra parte, en la Observación No. 7 se describe una debilidad encontrada en relación con la consecución de la información para la presente conformidad.

Conformidad No. 6

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Tema: Implementación de controles definidos en la Declaración de Aplicabilidad

Criterio: Documento Maestro Modelo de Seguridad y Privacidad de la Información MSPI

8.1 Planificación e implementación
Evidencia de la implementación de los controles de seguridad y privacidad de la información

Condición:

Se evidencia que la entidad cuenta con el documento Declaración de aplicabilidad, el cual da cumplimiento al literal i) del numeral 7 del MSPI, este documento fue enviado por el jefe de la Oficina de Tecnologías de la Información el día 23/05/2024, este documento es el que permite conocer el estado de implementación de los controles en la entidad.

De la declaración de aplicabilidad se evidencia que de los 114 controles registrados la entidad tiene implementados 102, esto resulta de la revisión de la casilla denominada Control Implementado.

Tomando como base este documento de esos 102 controles implementados se tomó una muestra del 57.8% es decir se revisaron 59 controles.

El detalle de los resultados de la verificación de cada control se encuentra en el *Anexo 1. Aplicabilidad de los controles de Seguridad de la Información.*

Se concluye que los 59 controles tomados como muestra cuentan con algún registro o acción que soporta su implementación; no obstante, se evidencian aspectos por mejorar por lo que en el mencionado documento se registran recomendaciones específicas según el control que se pueden filtrar en la columna G del Anexo 1.

HALLAZGOS DE LA AUDITORÍA:

TEMA: Diagnostico MSPI

CRITERIO: Documento Marco – Modelo de Seguridad y Privacidad de la Información
No. 6 Diagnostico

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación, y actualizarlo posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño será incluido como un insumo, en la fase de mejoramiento continuo.

CONDICIÓN:

El día 14/05/2024 se recibió por correo electrónico el documento de autodiagnóstico denominado *Instrumento_Evaluación_MSPI,* dicho documento consta de las siguientes hojas, las cuales al ser analizadas recogen la siguiente información relevante en el proceso de autodiagnóstico y presentan algunas inconsistencias detalladas en la siguiente tabla:

Tabla No. 3 Análisis del autodiagnóstico

Nombre de la hoja	Información relevante	Campos que no están diligenciados o tienen información inconsistente
Portada	Cuenta con una tabla que permite calcular el promedio de evaluación de los controles que	La fecha de evaluación se registra como 30 julio de 2023 lo cual no es consistente, dado

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

	tiene como resultado una calificación de 44 sobre 100. El porcentaje de avance en la vigencia 2020 calculado para el ciclo PHVA es de 36%	que las tablas evalúan criterios de la vigencia 2020.
Levantamiento de Info.	Sin diligenciar	Sin diligenciar
Áreas involucradas	Se compone de las columnas responsable, tema y funcionario.	No esta diligenciada la columna funcionario, así como tampoco están relacionados los procesos de la entidad
Administrativa	Las columnas definidas buscan identificar el cumplimiento administrativo de los ítems de seguridad de la información, tanto en la ISO 27001, en el MSPI y Ciberseguridad; así mismo cuenta con la columna prueba que indica qué debe tener o cómo evaluar el cumplimiento, la columna evidencia, brecha, nivel de cumplimiento y recomendación. Únicamente se evidencia diligenciada la columna nivel de cumplimiento	No están diligenciadas las columnas indispensables para determinar el grado de madurez del modelo como lo son evidencia y brecha.
Técnica	Las columnas definidas buscan identificar el cumplimiento técnico de los ítems de seguridad de la información, tanto en la ISO 27001, en el MSPI y Ciberseguridad; así mismo cuenta con la columna prueba que indica qué debe tener o cómo evaluar el cumplimiento, la columna evidencia, brecha, nivel de cumplimiento y recomendación. Únicamente se evidencia diligenciada la columna nivel de cumplimiento	No están diligenciadas las columnas indispensables para determinar el grado de madurez del modelo como lo son evidencia y brecha.
PHVA	Las columnas definidas buscan identificar el cumplimiento de las etapas del ciclo PHVA, así mismo cuenta con la columna prueba que indica qué debe tener o cómo evaluar el cumplimiento, la columna evidencia, brecha, nivel de cumplimiento y recomendación. Únicamente se evidencia diligenciada la columna nivel de cumplimiento	No están diligenciadas las columnas indispensables para determinar el grado de implementación del ciclo PHVA como lo son evidencia y brecha.
Madurez	Columna formulada con datos de nivel de cumplimiento	No es claro el resultado dado que las columnas de resultado son dos: Nivel y Cumple; en todos los campos de cumple el resultado es FALSO El otro campo es Nivel de Madurez alcanzado y el resultado es NO ALCANZA NIVEL INICIAL

Fuente: Elaboración propia

HALLAZGO N°1

Revisado el documento de autodiagnóstico presentado el día 14/05/2024 por el grupo auditado se identificaron las siguientes debilidades:

- Se evidencia que el mismo no cumple con los mínimos requeridos tal y cómo se describe en la tabla No.1 donde se observa que campos relevantes como responsable, evidencia y brecha no fueron diligenciados.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- Se evidencia que no es posible establecer si este documento es el inicial, lo anterior dado que en el contenido al parecer se evalúan los criterios en la vigencia 2020 (antes de la expedición del MSPI) pero en la fecha de elaboración registra julio de 2023, dato que tampoco es consistente pues en la hoja denominada *Portada*, solo están datos de la vigencia 2020

Esta situación permite concluir que se incumple lo establecido en el No. 6 Diagnostico del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic.

Dichas debilidades fueron socializadas por correo electrónico del 14/05/2024

CAUSAS:

- Debilidades en la gestión del conocimiento al interior de la Oficina de Tecnologías de la Información, aunado a los cambios del personal que impiden la continuidad de los procesos o cumplimiento de actividades previamente formuladas.

CONSECUENCIAS:

- Falta de certeza en el estado actual de las brechas que tiene la entidad para la implementación del Modelo de Seguridad y Privacidad de la Información
- Reprocesos y demoras en la implementación de todos los aspectos incluidos en el Modelo de Seguridad y Privacidad de la Información

RECOMENDACIONES:

- Actualizar el autodiagnóstico del MSPI

Respuesta del equipo auditado antes del cierre de auditoría:

El día 24/07/2024 se recibe respuesta de la Oficina de Tecnologías de la Información con radicado 3-2024-1304, donde indican que no hay observaciones o aclaraciones frente al hallazgo.

Análisis OCI de los argumentos y aportes del proceso auditado

Dado que el proceso acepta el hallazgo, no hay comentarios adicionales

Resultado del Hallazgo: SE RATIFICA

TEMA: Roles y Responsabilidades

CRITERIO: Documento Marco – Modelo de Seguridad y Privacidad de la Información

7.2.3 Roles y responsabilidades

Articular con las áreas o dependencias de la entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño, para que sean aprobados y comunicados dentro de la entidad.

Se debe delegar a un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI; si el cargo no existe en la entidad deberá ser delegado por acto

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz.

Hay que asegurar que los funcionarios de la entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI

CONDICIÓN:

El día 14/05/2024 se recibió por correo electrónico enviado por la Oficina de Tecnologías de la Información el documento denominado MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN, el cual fue aprobado en Comité Institucional de Gestión y Desempeño el día 16/08/2023, tal y como consta en el numeral 8 del acta de dicha sesión. En el numeral 5 del documento aprobado se incluye el siguiente capítulo:

"5.2.1. Roles y responsabilidades
Todo aquel que tenga acceso a la información de la LOTERÍA DE BOGOTÁ, será responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este documento; entre ellos están: funcionarios, contratistas, entes de control, proveedores y visitantes.
El incumplimiento de procedimientos o políticas de seguridad de la información por no atención de los comunicados oficiales no exime al funcionario, contratista, proveedor o visitante de las medidas que pueda tomar la LOTERÍA DE BOGOTÁ, como se menciona en la sección 6.4.3 de este documento.
El Oficial de Seguridad de la Información (OSI), asumirá la responsabilidad por el desarrollo e implementación de la seguridad de la información, comprobará el cumplimiento de las políticas, en caso de requerirse prestará asesoría a todo aquel que maneje información de la entidad, coordinará las actividades de la gestión de riesgos de la seguridad de la información con el apoyo de la oficina de planeación estratégica de la Lotería de Bogotá, para la identificación de controles y reportará al Comité Institucional de Gestión y Desempeño de la Lotería de Bogotá."

Por otra parte, en la mesa de trabajo No. 2 el jefe de la Oficina de Tecnologías de la Información informa que la entidad contrató al profesional responsable de liderar los temas de seguridad de la información mediante contrato de prestación de servicios 36 de 2024 cuyo objeto es "PRESTAR SERVICIOS PROFESIONALES PARA LA FORMULACIÓN, IMPLEMENTACIÓN, ACTUALIZACIÓN Y ACOMPAÑAMIENTO A PROCESOS DE TECNOLOGÍA RELATIVOS AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA LOTERÍA DE BOGOTA"

Por otra parte, Mintic expidió un documento guía denominado Roles y Responsabilidades MSPI, dicho documento establece en detalle los roles y responsabilidades para el responsable de Seguridad de la Información, Comité Institucional de Gestión y Desempeño Institucional, Oficina asesora Jurídica, Gestión del Talento Humano y Control Interno.

Se concluye que la inclusión del capítulo No. 5 en la Política de Seguridad de la Información no es suficiente para dar por cumplido el criterio. Adicional a ello la entidad no ha expedido el acto administrativo de nombramiento del Oficial de Seguridad de la Información.

HALLAZGO N°2

Revisado el documento MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN versión 4 del año 2023 se identificaron las siguientes debilidades:

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- Se evidencia que no se han definido de manera específica los Roles y Responsabilidades del MSPI para el responsable de Seguridad de la Información, el Comité Institucional de Gestión y Desempeño Institucional, la Oficina Asesora Jurídica, la Unidad de Talento Humano y la Oficina de Control Interno. lo anterior denota incumplimiento del numeral 7.2.3 Roles y responsabilidades del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021

- Se evidencia que no se ha expedido el acto administrativo de nombramiento de un profesional que dependa de un área estratégica, que no sea la Oficina de Tecnologías de la Información, que deberá ser incluida como miembro del Comité de Gestión institucional con voz y voto y en el Comité de Coordinación Institucional de Control Interno con voz; lo anterior denota incumplimiento del numeral 7.2.3 Roles y responsabilidades del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021

Dichas debilidades fueron socializadas por correo electrónico del 23/05/2024

CAUSAS:

- Falta de definición y análisis de los cargos existentes en planta de personal con el fin de determinar si existe el perfil para ocupar el cargo de Oficial de Seguridad de la Información.

CONSECUENCIAS:

- Indebida segregación de funciones dado que es necesario que el Oficial de Seguridad no dependa de la Oficina de Tecnologías de la Información, sino de un proceso estratégico que le permita liderar el MSPI involucrando todas las áreas que sean necesarias para la adecuada implementación.

RECOMENDACIONES:

- Realizar el análisis de la planta de personal actual y definir si existe actualmente un profesional que tenga el perfil idóneo para ser designado como Oficial de Seguridad de la Información, en caso de no contar con ese perfil, gestionar la ampliación de la planta de personal.

Respuesta del equipo auditado antes del cierre de auditoría:

El día 24/07/2024 se recibe respuesta de la Oficina de Tecnologías de la Información con radicado 3-2024-1304, donde indican que no hay observaciones o aclaraciones frente al hallazgo.

Análisis OCI de los argumentos y aportes del proceso auditado

Dado que el proceso acepta el hallazgo, no hay comentarios adicionales

Resultado del Hallazgo: SE RATIFICA

TEMA: Identificación de activos de información e infraestructura critica

CRITERIO: Documento Marco – Modelo de Seguridad y Privacidad de la Información

7.3.1 Identificación de activos de información e infraestructura critica

Las entidades deben definir y aplicar un proceso de identificación y clasificación de la información, que permita:

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

• Determinar o identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.
• Clasificar los activos de información de acuerdo a los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.
• Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso

CONDICIÓN:

El día 20/05/2024 se recibió de la Oficina de Tecnologías de la Información el documento DOC340-578-1 GUIA PARA LA IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, el cual fue aprobado el día 17 de mayo de 2023 en el Comité Institucional de Gestión y Desempeño. Dicho documento tiene por objetivo "Brindar orientaciones necesarias a la Lotería de Bogotá a través de una metodología para identificar, clasificar, valorar y gestionar los activos de información de manera que sirvan de insumo para la gestión de riesgos de Seguridad de la Información en la institución".

Asimismo, se recibieron siete (7) formatos código FRO-340-577 1 Inventario de Activos de Información los cuales corresponden a diez (10) procesos citados a continuación:

1. Planeación y Direccionamiento Estratégico
2. Atención y Servicio al Cliente
3. (2 procesos) Cumplimiento y Gestión LA/FT/FPADM y Anticorrupción y Antisoborno (SGAS)
4. Explotación de Juegos de Suerte y Azar
5. Gestión de las Tecnologías y la Información
6. Evaluación Independiente a la Gestión
7. (3 procesos) Gestión de Bienes y Servicios, Gestión del Talento Humano y Gestión Jurídica. Se observa que al filtrar Gestión del Talento esta dependencia solo tiene 2 activos que en su denominación es el mismo (Créditos Modalidad Adquisición, Construcción, Abono o Liberación de Hipoteca, Mejoramiento Reparación de Vivienda).

Los inventarios antes mencionados cuentan con la identificación de activos, la relación con las Tablas de Retención Documental, valoración del activo, referencia a los aspectos de protección de datos personales, alineación a la Ley de Transparencia; esto permite concluir que se realizó la clasificación de los activos de información de acuerdo a los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad.

Revisado el Mapa de Procesos de la entidad publicado en el link: https://loteriadebogota.com/procedimientos-2/ donde se observa 17 procesos documentados, se evidencia que de los siguientes siete (7) procesos no se cuenta, a la fecha, con el Inventario de Activos de Información:

1. Gestión de Comunicaciones
2. Gestión de Recaudo
3. Control, Inspección y Fiscalización
4. Gestión Financiera y Contable
5. Gestión Documental
6. Control Interno Disciplinario
7. Protección de Datos Personales

HALLAZGO N°3 (HALLAZGOS NÚMEROS 3 Y 4 DEL INFORME PRELIMINAR QUE SE UNIFICAN Y REGISTRA COMO HALLAZGO NRO. 3 DE ESTE INFORME FINAL)

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Revisada la información recibida por parte de la Oficina de Tecnologías de la Información el día 20/05/2024 que corresponde al formato de Inventario de Activos de Información de 10 de los 17 procesos que tiene la entidad, se identificaron las siguientes debilidades:

- Se evidencia que para el 41% de los procesos (Gestión de Comunicaciones, Gestión de Recaudo, Control, Inspección y Fiscalización, Gestión Financiera y Contable, Gestión Documental, Control Interno Disciplinario y Protección de Datos Personales), no se cuenta con Inventario de Activos de Información; esto incumple lo establecido en el numeral 7.3.1 Identificación de activos de información e infraestructura critica del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic.

- El inventario del proceso Gestión del Talento Humano solo cuenta con 1 activo de información definido. Situación que no es consistente con las diferentes funciones que ejecuta la unidad y de las cuales se podrían identificar como activos de información tales como nómina, situaciones administrativas del personal de planta, actividades de capacitación y bienestar, temas de seguridad y salud en el trabajo, entre otros.

Dichas debilidades fueron socializadas por medio de correo electrónico el día 23/05/2024

CAUSAS:

- Falta de recursos asignados por la entidad para adelantar las actividades de implementación del MSPI dado que la implementación implica múltiples actividades que una sola persona contratada no alcanza a ejecutarlas de manera eficiente.

CONSECUENCIAS:

- Demora en la implementación de las políticas de administración de riesgos de seguridad de la información y la formulación de planes para tratamiento de los riesgos asociados a activos críticos de seguridad de la información.

RECOMENDACIONES:

- Definir un plan de choque a ejecutarse en la vigencia 2024 que permita el levantamiento del Inventario de Activos de los siete (7) procesos que aún no han adelantado la identificación.

Respuesta del equipo auditado antes del cierre de auditoría:

El día 24/07/2024 se recibe respuesta de la Oficina de Tecnologías de la Información con radicado 3-2024-1304, donde solicitan "*se unifiquen los hallazgos 3 y 4, teniendo en cuenta que, la metodología de riesgos de seguridad de la información tiene como base la identificación calificación de los activos de información, ya fue parte de la calificación que tenga cada activo. En este sentido, no se podría cumplir con las acciones de mejora del hallazgo 4, hasta tener las del hallazgo 3, ya que hacen parte de una misma metodología. Lo anterior se puede apreciar según lo establecido, en la Guía para la administración del Riesgo y el diseño de controles en entidades públicas del Departamento de Función Pública, en donde se tiene incorporado en su capítulo # 6 lineamientos para riesgos de seguridad de la información, lo relacionado con la identificación de activos, en su apartado 6.1. "… como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso". Así mismo, en el Documento maestro del MSPSI, en su capítulo 7.3.2 se tiene como entrada para la valoración de riesgos, el inventario de activos de información. Por otro lado, en la planeación de actividades de la entidad, se puede apreciar que en el plan de Seguridad y*

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Privacidad de la Información de 2024 aprobado y publicado por la entidad, que definió que la publicación de sus activos de información se terminará el próximo 31 de diciembre de 2024."

Análisis OCI de los argumentos y aportes del proceso auditado

Dado que efectivamente el proceso de identificación de riesgos de seguridad de la información va directamente relacionado con la identificación de activos de información, es posible la unificación del hallazgo. No obstante, es indispensable que en el plan de mejoramiento se formulen acciones específicas con mediciones y productos independientes para las situaciones citadas en el presente informe para cada uno de los temas.

Resultado del Hallazgo: SE UNIFICA quedando con la siguiente redacción:

HALLAZGO No. 3

Revisada la información recibida por parte de la Oficina de Tecnologías de la Información el día 20/05/2024 que corresponde al formato de Inventario de Activos de Información de 10 de los 17 procesos que tiene la entidad, y analizada la Política de Administración de Riesgo de la entidad publicada en la página web a la fecha (19/07/2024) y teniendo en cuenta la información recibida en la mesa de trabajo realizada con los profesionales de la Oficina de Tecnologías de la Información el día 21/05/2024, se identificaron las siguientes debilidades:

- Se evidencia que para el 41% de los procesos (Gestión de Comunicaciones, Gestión de Recaudo, Control, Inspección y Fiscalización, Gestión Financiera y Contable, Gestión Documental, Control Interno Disciplinario y Protección de Datos Personales), no se cuenta con Inventario de Activos de Información; esto incumple lo establecido en el numeral 7.3.1 Identificación de activos de información e infraestructura critica del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic.

- El inventario del proceso Gestión del Talento Humano solo cuenta con 1 activo de información definido. Situación que no es consistente con las diferentes funciones que ejecuta la unidad y de las cuales se podrían identificar como activos de información tales como nómina, situaciones administrativas del personal de planta, actividades de capacitación y bienestar, temas de seguridad y salud en el trabajo, entre otros.

- Se evidencia que la política de administración de riesgos de la entidad no tiene establecidos los lineamientos específicos para la identificación y tratamiento de riesgos de seguridad de la información.

- Se evidencia que la entidad no ha aplicado el tratamiento de riesgos de la seguridad de la información

Lo anterior incumple los numerales 7.3.1 Identificación de activos de información e infraestructura critica, 7.3.2 Valoración de los riesgos de seguridad de la información y 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic.

TEMA: Valoración y tratamiento de los riesgos de seguridad de la información

CRITERIO: Documento Marco – Modelo de Seguridad y Privacidad de la Información

Criterio 1:
7.3.2 Valoración de los riesgos de seguridad de la información

Las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita:

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

• Identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI.
• Identificar los dueños de los riesgos.
• Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.
• Determinar el apetito de riesgos definido por la entidad
• Establecer criterios de aceptación de los riesgos.
• Aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la perdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance.
• Determinar los niveles de riesgo.
• Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral.
• Priorización de los riesgos analizados para su tratamiento.

Criterio 2
7.3.3 Plan de tratamiento de los riesgos de seguridad de la información

La entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:

• Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
• Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.
• Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad.
• Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

CONDICIÓN:

Se programa y sesiona mesa de trabajo, entre la auditora líder y los profesionales de la Oficina de Tecnologías de la Información el día 21/05/2024 donde se identifica que la entidad a la fecha ha adelantado acciones conducentes al cumplimiento de los criterios citados, como lo es la aprobación de la Política de Seguridad de la Información y los avances en cuanto a identificación y clasificación de activos de información.

No obstante, a la fecha no se ha realizado el ajuste de la Política de Administración de Riesgo de la entidad, la cual esta publicada en su última versión de noviembre de 2023 en el link: https://loteriadebogota.com/wp-content/uploads/POLITICA-DE-ADMINISTRACION-DEL-RIESGO-2023-V4-15-11-2023.pdf, la cual debe contener específicamente los lineamientos del DAFP contemplados en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, capitulo 6 Lineamientos riesgos de seguridad de la información, la cual fue publicada en noviembre de 2022.

Teniendo en cuenta que la política de riesgos de la entidad no ha sido actualizada tampoco se cuenta con la valoración y el plan de tratamiento de los riesgos de seguridad de la información.

La Oficina de Planeación por medio de correo electrónico del día 18/07/2024 aclaró que la entidad generó una nueva versión de la Política de Administración de Riesgo en Junio de 2024, la cual fue revisada y se evidencian ajustes en el numeral *6. Responsabilidad frente al riesgo* que indica que el encargado de evaluar el cumplimiento de los controles asociados a las Políticas de Seguridad de la Información es el Oficial de seguridad de la información o quien haga sus veces; por otra parte, se incluye en el numeral *14. Accionar frente*

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

a riesgos materializados, las actividades a seguir por parte de los líderes de proceso en caso de materializarse un riesgo de seguridad de la información. No obstante, dicho documento no contiene los lineamientos del DAFP contemplados en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, capitulo 6 Lineamientos riesgos de seguridad de la información, la cual fue publicada en noviembre de 2022.

HALLAZGO N°4 (HALLAZGOS NÚMEROS 3 Y 4 DEL INFORME PRELIMINAR QUE SE UNIFICAN Y REGISTRA COMO HALLAZGO NRO. 3 EN ESTE INFORME FINAL)

Analizada la Política de Administración de Riesgo de la entidad publicada en la página web a la fecha (19/07/2024) y teniendo en cuenta la información recibida en la mesa de trabajo realizada con los profesionales de la Oficina de Tecnologías de la Información el día 21/05/2024, se identificaron las siguientes debilidades:

- Se evidencia que la política de administración de riesgos de la entidad no tiene establecidos los lineamientos específicos para la identificación y tratamiento de riesgos de seguridad de la información.
- Se evidencia que la entidad no ha aplicado el tratamiento de riesgos de la seguridad de la información

Lo anterior incumple los numerales 7.3.2 Valoración de los riesgos de seguridad de la información y 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic.

Dichas debilidades fueron socializadas a la Oficina de Tecnología de la Información por medio de correo electrónico el día 23/05/2024 y a la Oficina de Planeación el día 17/07/2024, quien por medio de correo electrónico del día 18/07/2024 aclaró que la entidad generó una nueva versión de la Política de Administración de Riesgo en Junio de 2024, en la cual según el control de cambios “Se incluyen lineamientos sobre gestión de riesgos fiscales, de igual modo, se actualizan los roles y responsabilidades de la segunda línea de defensa”.

CAUSAS:

- Falta de recursos asignados por la entidad para adelantar las actividades de implementación del MSPI dado que la implementación implica múltiples actividades que una sola persona contratada no alcanza a ejecutarlas de manera eficiente.

CONSECUENCIAS:

- Aumento en la posibilidad de materialización de riesgos por falta de definición de controles de seguridad de la información

RECOMENDACIONES:

- Gestionar recursos adicionales para la Oficina de Tecnologías de la Información para la implementación del MSPI que permitan en el menor tiempo posible actualizar la política de administración de riesgos

- Gestionar mesas de trabajo entre la Oficina de Tecnologías de la Información y la Oficina de Planeación para definir actividades, responsabilidades y tiempos para la actualización de la Política de Administración de Riesgos en la presente vigencia.

Respuesta del equipo auditado antes del cierre de auditoría:

El día 24/07/2024 se recibe respuesta de la Oficina de Tecnologías de la Información con radicado 3-2024-1304, donde solicitan “*se unifiquen los hallazgos 3 y 4, teniendo en cuenta que, la metodología de riesgos de*

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

seguridad de la información tiene como base la identificación calificación de los activos de información, ya fue parte de la calificación que tenga cada activo. En este sentido, no se podría cumplir con las acciones de mejora del hallazgo 4, hasta tener las del hallazgo 3, ya que hacen parte de una misma metodología. Lo anterior se puede apreciar según lo establecido, en la Guía para la administración del Riesgo y el diseño de controles en entidades públicas del Departamento de Función Pública, en donde se tiene incorporado en su capítulo # 6 lineamientos para riesgos de seguridad de la información, lo relacionado con la identificación de activos, en su apartado 6.1. "… como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso". Así mismo, en el Documento maestro del MSPSI, en su capítulo 7.3.2 se tiene como entrada para la valoración de riesgos, el inventario de activos de información. Por otro lado, en la planeación de actividades de la entidad, se puede apreciar que en el plan de Seguridad y Privacidad de la Información de 2024 aprobado y publicado por la entidad, que definió que la publicación de sus activos de información se terminará el próximo 31 de diciembre de 2024."

Análisis OCI de los argumentos y aportes del proceso auditado

Dado que efectivamente el proceso de identificación de riesgos de seguridad de la información va directamente relacionado con la identificación de activos de información, es posible la unificación del hallazgo. No obstante, es indispensable que en el plan de mejoramiento se formulen acciones específicas con mediciones y productos independientes para las situaciones citadas en el presente informe para cada uno de los temas.

Resultado del Hallazgo: SE UNIFICA y queda codificado como Hallazgo No. 3

TEMA: Partes Interesadas del MSPI

CRITERIO: Documento Marco – Modelo de Seguridad y Privacidad de la Información

7.1.2. Necesidades y expectativas de los interesados

Se deben determinar las partes interesadas internas o externas y personas, entidades u organizaciones que pueden influir directamente en la seguridad y privacidad de la información de la entidad o que puedan verse afectados en caso de que estas se vean comprometidas. Adicionalmente se deberán determinar las necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información. Las partes interesadas deberán incluir los requisitos legales, reglamentarios y contractuales.

CONDICIÓN:

El día 22/05/2024 se recibe por parte de la Oficina de Planeación el documento denominado Caracterización de Usuarios y Partes Interesadas, el mismo día se valida la publicación en el link: https://loteriadebogota.com/wp-content/uploads/Caracterizacion-de-partes-interesadas-2023-26-03-2024.pdf.

En relación con el cumplimiento del criterio y el contenido del documento se evidencia que se definen los siguientes objetivos específicos:

"2.2. Objetivos Específicos

- Identificar las necesidades, intereses, expectativas y preferencias de las Partes Interesadas para garantizar el efectivo ejercicio de sus derechos en la interacción con la Lotería de Bogotá.
- Optimizar los canales de comunicación actualmente disponibles para las partes interesadas.
- Identificar las características principales de cada grupo con el fin de orientar de forma más efectiva las distintas estrategias para la comunicación y la prestación del servicio.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- Construir información confiable sobre las partes interesadas con el fin de construir e implementar políticas organizacionales coherentes con la caracterización y comportamiento de las partes interesadas".

No obstante, teniendo en cuenta que el criterio evaluado indica que se deben determinar las partes interesadas internas o externas y personas, entidades u organizaciones **que pueden influir directamente en la seguridad y privacidad de la información de la entidad** o que puedan verse afectados en caso de que estas se vean comprometidas, el documento aprobado no cumple con el lineamiento, dado que no incorpora las partes interesadas antes citadas.

Por otra parte, el MSPI también define que es necesario "determinar las necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información. Las partes interesadas **deberán incluir los requisitos legales, reglamentarios y contractuales**"; actividad que tampoco se refleja en el soporte entregado.

HALLAZGO N° 4

Revisado el documento denominado Caracterización de Usuarios y Partes Interesadas, recibido el día 22/05/2024 por parte de la Oficina de Planeación, se evidencia que incumple lo establecido en el numeral 7.1.2. Necesidades y expectativas de los interesados del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic, dado que en el mismo no se identifican expresamente las partes internas y externas que pueden influir directamente en la seguridad y privacidad de la información, así como tampoco se determinan los requisitos legales, reglamentarios y contractuales de dichas partes.

Dicha debilidad fue socializada por medio del correo electrónico enviado a la Oficina Asesora de Planeación el día 28/05/2024.

CAUSAS:

- Falta de recursos asignados por la entidad a la Oficina de Tecnologías de la Información para adelantar las actividades de implementación del MSPI dado que la implementación implica múltiples actividades que una sola persona contratada en Tecnología, quien debe proveer la información para el criterio objeto de evaluación, no alcanza a ejecutarlas de manera eficiente.
- Falta de gestión por parte de la Oficina de Planeación para actualizar la Caracterización de Usuarios y Partes Interesadas en aspectos de seguridad de la información.

CONSECUENCIAS:

- Inadecuada identificación de riesgos e implementación de controles deficientes por falta de conocimiento de las partes interesadas que influyen directamente en la seguridad y privacidad de la información.

RECOMENDACIONES:

- Gestionar mesas de trabajo entre la Oficina de Tecnologías de la Información y la Oficina de Planeación para definir actividades, responsabilidades y tiempos para la actualización de la Caracterización de Usuarios y Partes Interesadas
- Actualizar el documento de Caracterización de Usuarios y Partes Interesadas
- Presentar el documento al Comité Institucional de Gestión y Desempeño para la respectiva aprobación e implementación.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Respuesta del equipo auditado antes del cierre de auditoría:

El día 24/07/2024 se recibe respuesta de la Oficina de Tecnologías de la Información con radicado 3-2024-1304, donde indican que no hay observaciones o aclaraciones frente al hallazgo. Así mismo el mismo día se recibe respuesta verbal por parte del jefe de la Oficina de Planeación indicado que aceptan el hallazgo.

Análisis OCI de los argumentos y aportes del proceso auditado

Dado que el proceso acepta el hallazgo, no hay comentarios adicionales

Resultado del Hallazgo: SE RATIFICA

TEMA: Funciones del Comité Institucional de Gestión y Desempeño frente al MSPI

CRITERIO: Documento Marco – Modelo de Seguridad y Privacidad de la Información

7.2.1 Liderazgo y Compromiso

La entidad debe incluir dentro del comité institucional de gestión y desempeño o quien haga sus veces, las funciones relacionadas con idad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, por medio de un acto administrativo.
(…)
Documento a verificar: Acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.

7.2.2 Política de seguridad y privacidad de la información
Se debe establecer en la política de seguridad y privacidad de la información, que establezca el enfoque de la entidad, para ello debe tener en cuenta: (…) Ser incluidos y aprobados los temas de seguridad de la información y seguridad digital en el Comité Gestión y Desempeño Institucional, modificando el acto administrativo de conformación de este, aprobado por el mismo comité y expedido por el nominador o máxima autoridad de la entidad.

CONDICIÓN:

El día 27/05/2024 se recibe por parte de la Oficina de Planeación la Resolución No. 68 de 2018 “Por la cual se integra y se establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Lotería de Bogotá”, la cual en el artículo 5 establece:

“Funciones del Comité Institucional de Gestión y Desempeño: Son funciones del Comité Institucional de Gestión y Desempeño de la Lotería de Bogotá las siguientes:
(…) 12. Desarrollas las funciones asignadas a los comités institucionales que no tienen origen legal, así:
(…) 12.3. Comité de Sistemas y Seguridad de la Información: Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información al interior de la Lotería de Bogotá (…)

También se recibe la Resolución No. 107 de 2023 “Por la cual se integra y se adopta el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Lotería de Bogotá” la cual en el artículo 19 deroga la Resolución 68 de 2018. En cuanto a las funciones del mencionado comité el artículo 5 no establece ninguna especifica de los temas de temas de seguridad de la información y seguridad digital. Sin embargo, se incluye la función No. 13. Estudiar y aprobar el Plan Estratégico de Tecnología y Sistemas de Información PETI

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

propuesto por el área correspondiente, la cual podría ser aplicable al criterio, siempre y cuando la entidad en el PETI incorpore integralmente todo lo definido en el MSPI.

El día 28/05/2024 se realizó consulta en el SHAREPOINT compartido por la Oficina de Planeación donde reposa el PETI para la vigencia 2024 y se evidencia que dicho documento no abarca los temas de seguridad de la información y seguridad digital que establece el MSPI. Por lo tanto, no es posible concluir que con la función No. 13 (Estudiar y aprobar el Plan Estratégico de Tecnología y Sistemas de Información PETI), se de cumplimiento al numeral 7.1.1. del MSPI que define que el comité institucional de gestión y desempeño debe tener las funciones relacionadas con seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, y deben estar definidas por medio de un acto administrativo

Lo anterior permite concluir que la entidad no ha expedido el acto administrativo modificando las funciones del Comité Institucional de Gestión y Desempeño, incorporando las relacionadas con seguridad y privacidad de la información, que permitan adoptar, implementar, mantener y mejorar continuamente el MSPI.

HALLAZGO N°5

Revisada la información recibida el día 27/05/2024 por parte de la Oficina de Planeación en relación con las resoluciones de creación y modificación de la conformación del Comité Institucional de Gestión y Desempeño, y analizada la resolución vigente No. 107 de 2023 *"Por la cual se integra y se adopta el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Lotería de Bogotá"*, se evidencia que en el artículo *5° Funciones*, no se incorporan las funciones relacionadas con seguridad y privacidad de la información, lo que conlleva al incumplimiento de los numerales 7.2.1 Liderazgo y Compromiso y 7.2.2 Política de seguridad y privacidad de la información del documento maestro Modelo de Seguridad y Privacidad de la Información expedido en la vigencia 2021 por Mintic.

Dicha debilidad fue socializada por medio del correo electrónico enviado a la Oficina Asesora de Planeación el día 28/05/2024

CAUSAS:

- Indebida revisión de la Resolución 107 de 2023, dado que derogó el acto administrativo expedido por la entidad en la vigencia 2018 que incluía de manera precisa las funciones relacionadas con seguridad y privacidad de la información.

CONSECUENCIAS:

- Reproceso en la expedición de actos administrativos asociados a las funciones del Comité Institucional de Gestión y Desempeño

RECOMENDACIONES:

- Modificar el acto administrativo que define las funciones del Comité Institucional de Gestión y Desempeño incorporando las asociadas a seguridad y privacidad de la información.

Respuesta del equipo auditado antes del cierre de auditoría:

El día 24/07/2024 se recibe respuesta de la Oficina de Tecnologías de la Información con radicado 3-2024-1304, donde indican que no hay observaciones o aclaraciones frente al hallazgo. Así mismo el mismo día se recibe respuesta verbal por parte del jefe de la Oficina de Planeación indicado que aceptan el hallazgo.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Análisis OCI de los argumentos y aportes del proceso auditado

Dado que el proceso acepta el hallazgo, no hay comentarios adicionales

Resultado del Hallazgo: SE RATIFICA

TEMA: Competencia, toma de conciencia y comunicación

CRITERIO: Documento Marco – Modelo de Seguridad y Privacidad de la Información

7.4.2 Competencia, toma de conciencia y comunicación

La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para:

• Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
• Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.
• Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información.
• Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.

Documentos a revisar:
Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC.
• Plan de comunicaciones del modelo de seguridad y privacidad de la información.

CONDICIÓN:

Para validar el criterio se enviaron los requerimientos No. 9 a la Unidad de Talento Humano, relacionado con capacitaciones y formación en temas del MSPI y el No. 10 a Comunicaciones relacionado con la comunicación del MSPI. La consolidación de los resultados se presenta por cada tema incluido en el criterio, así:

a. Toma de conciencia

El día 04/06/2024 se recibió respuesta de la Unidad de Talento Humano en relación a las capacitaciones o procesos de formación adelantados durante el 2023 y 2024 en temas de seguridad y privacidad de la información que son:

- El 27 de abril de 2023, capacitación “Introducción a la Ciberseguridad - Lotería de Bogotá”. Según lista de asistencia participaron 39 personas
- El 01 de noviembre de 2023, se realizó capacitación de “Incidentes de Seguridad de la Información”. No se recibió soporte de ejecución, por lo tanto, no fue posible determinar el número de asistentes
- El 28 de mayo de 2024 se realizó capacitación “Riesgos de seguridad de la información”. Según lista de asistencia participaron 34 personas

Asimismo, la Unidad de Talento humano informa que en el Plan Institucional de Capacitación se tienen programadas las siguientes capacitaciones para el resto de la vigencia 2024:

- “Eventos, incidentes de seguridad de la información” se encuentra proyectada para su realización en el mes de septiembre de 2024.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- "Gobierno para la transformación Digital y Cibercultura para la alta dirección" se encuentra proyectado para octubre de 2024

Por otra parte y con el fin de realizar un diagnostico del tema en la entidad, el auditor elaboró y envió por medio de formato FORMS el día 11/06/2024 la encuesta denominada *Seguridad y Privacidad de la Información* a todos los colaboradores de la entidad. Dicha encuesta fue contestada por 37 personas. A continuación, se realiza un consolidado y análisis de los resultados por cada pregunta:

Tabla No. 4 Análisis del resultado de la encuesta de Seguridad de la Información

Pregunta	Análisis
1 y 2 Nombre, dependencia y tipo de vinculación	Fue contestada por 37 personas, de Atención al Cliente no contestó nadie y de Dirección General, Planeación, Jurídica y Unidad de Apuestas solo contestó una (1) persona.
3 Tipo de vinculación	Contestaron 14 trabajadores oficiales, 6 empleados públicos y 17 contratistas
4 Conoce la Política de Seguridad y Privacidad de la Información de la Lotería de Bogotá	34 personas si la conocen, 1 no la conoce y 2 no sabe/no responde
5 Registre en el siguiente espacio algún lineamiento que aplique en sus labores o actividades y esté relacionado con Seguridad de la Información	34 personas si registraron de manera coherente políticas de seguridad de la información, las 3 restantes no registraron nada.
6. Ha recibido en el último año alguna capacitación o sensibilización relacionada con la Política de Seguridad y Privacidad de la Información	28 personas si han recibido capacitaciones, 4 no han recibido y 5 no sabe/no responde
7. Registre en el siguiente espacio si ha realizado algún curso o proceso de formación presencial o virtual relacionado con el Modelo de Seguridad y Privacidad de la Información MSPI, adoptado por el Gobierno Nacional.	10 personas manifestaron que si han realizado algún curso o proceso de formación del tema, los 17 restantes contestaron que no.
8 Utiliza memorias USB o discos duros personales en los equipos de la entidad	35 personas contestaron que no y 2 que si; al revisar las personas que utilizan memoria tienen cargos de alta dirección o coordinación
9. Trae a la entidad su computador portátil personal y se conecta a la Red de la Entidad	30 personas no lo traen y 7 si
10. Favor colocar el nombre del Antivirus que utiliza en su computador portátil personal	Las 7 personas que traen el equipo portátil, cuentan con antivirus, en su mayoría McAfee®
11. Conoce la política de Escritorio Limpio del Modelo de Seguridad y Privacidad de la Información MSPI	27 personas si conocen la política, 9 no la conocen y 1 no sabe/no responde
12. En lo que conoce, considera que la entidad ha proporcionado los recursos necesarios para implementar políticas de seguridad y privacidad de la información	20 personas consideran que la entidad si ha proporcionado recursos, 7 que no ha proporcionado recursos y 10 no saben
13. Justifique la respuesta del punto 12	La mayoría de las personas asocian los recursos a las capacitaciones y charlas recibidas, algunos manifiestan que aunque hay documentos en la práctica falta mucho para que se apliquen, también consideran que faltan recursos humanos y tecnológicos para la debida implementación de la seguridad de la información.
14. Sabe usted si en el último año en la Entidad ha ocurrido alguna situación (evento) de seguridad de la información (perdida de datos, acceso no autorizado, perdida de expedientes, entre otros)	2 personas contestan que si, 21 que no y 14 no sabe/no responde
15. Especifique cuál situación se presentó	Las situaciones son: Se borro una carpeta del DRIVE y la segunda manifiesta que el asunto está en trámite disciplinario
16.Conoce el Oficial de Seguridad de la Información de la Lotería de Bogotá	22 personas si lo conocen, 11 no lo conocen y 5 no sabe/no responde
17.Mencione su nombre	De las 22 personas que marcaron que SI lo conocen, solo 13 lo identifican de manera correcta. Se observa una confusión con el anterior profesional que ya no está contratado y con la Oficial de Cumplimiento.

Fuente: Elaboración propia

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Lo anterior nos permite concluir que el numeral 7.4.2 Competencia, toma de conciencia y comunicación, en cuanto a toma de conciencia se cumple parcialmente pues el número de asistentes a las capacitaciones no es del 100% y según la encuesta de percepción hay aspectos que requieren mayor claridad.

b. Competencia

El día 04/06/2024 se recibió respuesta de la Unidad de Talento Humano a la pregunta ¿La Unidad de Talento Humano ha realizado algún diagnostico o tiene conocimiento si las personas que prestan sus servicios a la Lotería tienen conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información?, de la cual se puede concluir que:

- En la Resolución No 228 de 2022 del 30 de diciembre de 2022, "Por la cual se adopta el nuevo Manual Especifico de Funciones y Competencias Laborales para los Empleados Públicos de la Lotería de Bogotá", se encuentra asignada la función de: "Liderar la definición, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información de la entidad acorde al marco legal y articulado con la plataforma estratégica institucional".

- Talento Humano menciona que verificó que el Jefe de Oficina de Gestión Tecnológica e Innovación, en su hoja de vida presentó certificación ITIL, que es una guía de buenas prácticas para la gestión de servicios de tecnologías de la información (TI). La guía ITIL ha sido elaborada para abarcar toda la infraestructura, desarrollo y operaciones de TI y gestionarla hacia la mejora de la calidad del servicio.

- Se realizó la contratación por prestación de servicios de la persona que lidera el MSPI, el cual, de acuerdo a la certificación de idoneidad, emitida por la Jefe de la Unidad de Talento Humano, acredita Título de formación profesional como Especialista en Seguridad Información, expedido por la Universidad Piloto de Colombia, del 26 de junio de 2014.

Lo anterior nos permite concluir que el numeral 7.4.2 Competencia, toma de conciencia y comunicación, en cuanto a competencia se cumple.

c. Comunicación

El día 27/06/2024 se recibió repuesta del Subgerente Comercial y de Operaciones quien tiene a su cargo el área de comunicaciones quien respondió ante la pregunta planteada el día 30/05/2024 "*Se han identificado las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Mintic establece que Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo. Si la respuesta es SI, favor enviar los soportes*" que únicamente se han publicado algunas piezas comunicativas "*pero no se han generado acciones solicitadas*".

Lo anterior nos permite concluir que el numeral 7.4.2 Competencia, toma de conciencia y comunicación, en cuanto a comunicación no se cumple.

HALLAZGO N°6

Revisada la información recibida el día 4 y 27 de junio de 2024 por la Unidad de Talento Humano y la Subgerencia Comercial y de Operaciones, respectivamente, y analizados los resultados de la encuesta de percepción enviada a todos los colaboradores de la entidad el día 11 de junio de 2024 se evidencian las siguientes debilidades:

- No se ha involucrado al 100% de los funcionarios de la entidad en la implementación del MSPI, esto se concluye dado que solo 14 trabajadores oficiales diligenciaron la encuesta

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- Falta concientización de los colaboradores en cuanto al MSPI tal y como se evidencia en la Tabla No. No. 4
- No se ha realizado por parte de la Subgerencia Comercial y de Operaciones la identificación de necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información.

Lo anterior conlleva al incumplimiento del numeral 7.4.2 Competencia, toma de conciencia y comunicación Del Documento Marco – Modelo de Seguridad y Privacidad de la Información

Estas debilidades fueron socializadas por medio de correo electrónico a la Oficina de Tecnologías de la Información, Subgerencia Comercial y Unidad de Talento Humano el día 03/07/2024.

CAUSAS:

1. Desconocimiento de los lineamientos del MSPI por parte de otras áreas diferentes a la Oficina de Tecnologías y la Información tales como la Unidad de Talento Humano y la Subgerencia Comercial y de Operaciones, las cuales son responsables de implementar aspectos asociados con toma de conciencia y comunicación.

CONSECUENCIAS:

1. Ocurrencia de posibles eventos de seguridad de la información

RECOMENDACIONES:

1. Definir y documentar de manera específica los roles y responsabilidades de todas las áreas que tienen que ejecutar acciones conducentes a la efectiva implementación del MSPI
2. Socializar el documento marco de MSPI con los líderes de los procesos que tienen a cargo acciones a implementar.

Respuesta del equipo auditado antes del cierre de auditoría:

El día 24/07/2024 se recibe respuesta de la Oficina de Tecnologías de la Información con radicado 3-2024-1304, donde indican que no hay observaciones o aclaraciones frente al hallazgo. Las otras dependencias no enviaron respuesta por lo que se concluye que aceptan el hallazgo.

Análisis OCI de los argumentos y aportes del proceso auditado

Dado que el proceso acepta el hallazgo, no hay comentarios adicionales

Resultado del Hallazgo: SE RATIFICA

ANÁLISIS DE RIESGOS DEL PROCESO
En la presente auditoría no se revisó matriz de riesgo de la Oficina de Tecnologías de la Información, dado que la auditoría esta enfocada de manera a específica al Modelo de Seguridad y Privacidad de la Información MSPI, el cual incorpora el criterio de *Riesgos de Seguridad de la Información;* el resultado del análisis del tema quedó registrado en el hallazgo No. 4.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

OBSERVACIONES	RECOMENDACIONES
Observación 1 **Tema: Definición de la Política General de Seguridad y Privacidad de la Información** Revisado el documento publicado por la entidad en el aparte de políticas Link https://loteriadebogota.com/wp-content/uploads/MANUAL-PSI-16082023-Aprobado-CIGD-04-09-2023.pdf, se observa que si bien todo el documento en su integralidad, contiene los lineamientos y políticas que la entidad adopta en esta materia, no hay un párrafo o capítulo del documento que de manera sucinta detalle el quién, qué, por qué, cuándo y cómo se implementa la Política de Seguridad y Privacidad de la Información.	**Recomendación 1** **Tema: Definición de la Política General de Seguridad y Privacidad de la Información** Analizar la pertinencia de documentar un texto o párrafo en el manual publicado por la entidad que permita al lector conocer de manera sucinta, cuál es el compromiso de la entidad frente a la seguridad de la información, es decir, cuál es la Política General de Seguridad y Privacidad de la Información. Para esto puede servir de orientación un documento generado por Mintic en la vigencia 2016 denominado Guía 2 Definición de la Política General de Seguridad y Privacidad de la Información publicado en el link: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf
Observación 2 **Tema: Información asociada con el MSPI publicada en la web** Se realiza consulta en la página web el día 16/05/2024 y se observa que los siguientes ítems del link https://loteriadebogota.com/transparencia/, no cuentan con información actualizada: • 7.1.1 Registro de activos de información, tipo datos.Matrix excel anexo 6: Se publica matriz de 2016, 2017 y 2020 • 7.1.1 Registro de activos de información, tipo datos.Matrix excel anexo 6: Se publica matriz de 2016 • 10. MODELO DE SEGURIDAD DE LA INFORMACIÓN: Documento que en la portada define el nombre SISTEMA DE INFORMACIÓN INTEGRADO DE GESTIÓN DOCUMENTAL. Este documento fue aprobado por el Comité Institucional de Gestión y Desempeño el 31/01/2022 por la oficina Oficial de Cumplimiento.	**Recomendación 2** **Tema: Información asociada con el MSPI publicada en la web** Actualizar la información publicada en la página web
Observación 3 **Tema: Plan de Seguridad y Privacidad de la Información vigencias 2023 y 2024** El día 14/05/2024 se realizó la revisión de los planes de las vigencias 2023 y 2024 recibidos ese día por parte de la Oficina de Planeación.	**Tema: Plan de Seguridad y Privacidad de la Información vigencias 2023 y 2024** **Recomendación 3** Revisar y reformular las actividades del plan para la vigencia 2024, de tal manera que los indicadores que se formulen obedezcan a

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Plan de Seguridad y Privacidad de la Información 2023:

La revisión consistió en analizar la consistencia del reporte frente a la meta definida y validar los soportes de cada una de las seis (6) actividades, del análisis se observan las siguientes debilidades:

No.	Actividad	Meta	Observación OCI
1	Identificar los requisitos y necesidades en términos de seguridad de la información de las partes interesadas, entendidas como todos los actores que intervienen en la seguridad de la información (…)	Mesas de Trabajo y Documento Oficializado y Socializado	El soporte es un correo electrónico de 03/10/2023 donde el jefe de TI menciona que no tiene comentarios a l matriz de partes interesadas. En lo soportes no está ni la matriz, ni lo soportes de aprobación en Comité, ni lo soportes de socialización.
2	Identificar, analizar y documentar las brechas relacionadas con la NTC ISO IEC 27001:2022 y otros estándares y normas asociadas que apliquen a la Entidad.	Mesas de Trabajo y Documento Oficializado y Socializado	El soporte es un pantallazo de la Hoja del documento de Evaluación del MSP con fecha julio de 2023, pero que en s contenido la información es del 2020, ta y como se detalla en el hallazgo No. 1 d la auditoría El soporte no es consistente con l actividad definida, y no hay soporte d aprobación, oficialización y socialización
3	Proyectar y gestionar la oficialización de la Declaración de Aplicabilidad de los controles de seguridad de la información relacionados en el Anexo A de la NTC ISO IEC 27001:2022 y la NTC ISO IEC 27002:2022.	Mesas de Trabajo y Documento Oficializado y Socializado	Se evidencia archivo de declaración d aplicabilidad No hay soporte de aprobación oficialización y socialización
4	Actualizar y socializar la documentación asociada a la metodología de inventario y clasificación de activos de la información de la Entidad de acuerdo con las condiciones tecnológicas, las funcionales actuales de la Entidad, así como los lineamientos gubernamentales vigentes y las buenas prácticas internacionales.	Mesas de Trabajo y Documento Oficializado y Socializado	Se evidencia GUIA PARA LA IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN aprobad en Comité Institucional de Gestión Desempeño del 17/05/202 No hay soportes de socialización
5	Elaborar y/o actualizar la documentación asociada a seguridad de la información y ciberseguridad en el Sistema Integrado de Gestión.	Mesas de Trabajo y Documento Oficializado y Socializado	Se evidencia Politica de Seguridad de l INFORMACIÓN aprobada en Comit Institucional de Gestión y Desempeñ del 16/08/2023 No hay soportes de socialización
6	Realizar acciones orientadas al mejoramiento continuo de las capacidades tecnológicas (infraestructura y	Mesas de Trabajo y Documento Oficializado y Socializado	La definición del indicador no permit establecer si se cumplió o no, esto dad que realizar acciones de mejoramient es una actividad muy amplia y a meno que se defina específicamente cuále

actividades específicas y detalladas, que realmente se puedan medir de manera objetiva y precisa. Esta actividad debe ser realizada en conjunto con la Oficina de Planeación, posterior a la definición real de cumplimiento de las metas de la vigencia 2023.

Recomendación 4

Precisar el avance real de las acciones a diciembre 31 del plan de la vigencia 2023, así como completar los soportes de las mismas; este reporte debe obedecer al avance respecto del indicador y la meta definida.

Recomendación 5

Fortalecer el proceso de reporte por parte del área de tecnología, así como la revisión por parte de la Oficina de Planeación, dado que por lo observado en la auditoría se observa que es débil y no se toman a tiempo los correctivos para que los reportes trimestrales y los soportes sean consistentes con las actividades, indicadores y metas definidas.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

	servicios tecnológicos) de la Lotería de Bogotá, usando la innovación y las buenas prácticas en seguridad TIC.		acciones se van a ejecutar, el resultado del indicador no es preciso. Por otra parte, la meta define documento oficializado y socializado y no se evidencia registro de dicho documento.

Plan de Seguridad y Privacidad de la Información 2024:

La revisión consistió en analizar la consistencia del reporte frente a la meta definida y validar los soportes de cada una de las seis (6) actividades, del análisis se observan las siguientes debilidades:

No.	Actividad	Meta	Observación OCI
1	Actualizar y formalizar los requisitos y necesidades en términos de seguridad de la información de las partes interesadas, entendidas como todos los actores que intervienen en la seguridad de la información, tales como proveedores, usuarios internos, usuarios externos, entre otros, relacionadas con la misión y visión de la Entidad, así como las autoridades y grupos de interés de la Entidad.	Mesas de Trabajo y Documento Oficializado y Socializado	En su esencia la actividad es la mism de la vigencia 2023. Se evidenci debilidad en la formulación de lo planes dado que no permiten establece el alcance de las acciones para cad vigencia.
2	Identificar, analizar y documentar las brechas relacionadas con la norma ISO 27001 asociada al Modelo de Seguridad y Privacidad de la Información, Furag y Diagnostico de Datos Personales.	Mesas de Trabajo y Documento Oficializado y Socializado	En su esencia la actividad es la mism de la vigencia 2023. Se evidenci debilidad en la formulación de lo planes dado que no permiten establece el alcance de las acciones para cad vigencia.
3	Formalizar la Declaración de Aplicabilidad de los controles de seguridad de la información relacionados en el Anexo A de la ISO 27001 asociada al Modelo de Seguridad y Privacidad de la Información.	Mesas de Trabajo y Documento Oficializado y Socializado	En la vigencia 2023 estaba definida e la meta la actividad de oficializar socializar la declaración d aplicabilidad, es decir que est actividad, en teoría ya estab culminada. Se evidencia debilidad en la formulació de los planes dado que no permite establecer el alcance de las accione para cada vigencia.
4	Identificar, analizar y documentar las brechas relacionadas con la norma ISO 27001 asociada al Modelo de Seguridad y Privacidad de la Información, Furag y Diagnostico de Datos Personales.	Mesas de Trabajo y Documento Oficializado y Socializado	Es igual a la actividad No. 2 Se evidencia debilidad en la revisión d los planes tanto por la Oficina d Tecnología como por la Oficina d Planeación.
5	Elaborar y/o actualizar la documentación asociada a seguridad de la información y	Mesas de Trabajo y Documento	En su esencia la actividad es la mism de la vigencia 2023. Se evidenci debilidad en la formulación de lo planes dado que no permiten establece

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

	ciberseguridad en el Sistema Integrado de Gestión.	Oficializado y Socializado	el alcance de las acciones para cada vigencia.
6	Realizar análisis de vulnerabilidades	Informe ejecutivo y detallado	Sin reporte de avance
7	Publicar el registro de activos de información y el índice de información clasificada y reservada en la entidad.	Documentos Formalizados y Publicados en la Página Web y en Datos Abiertos	Sin reporte de avance

Observación 4
Tema: Declaración de Aplicabilidad

Se evidencia que la entidad cuenta con el documento Declaración de aplicabilidad, el cual da cumplimiento al literal i) del numeral 7 del MSPI, este documento fue enviado por el jefe de la Oficina de Tecnologías de la Información el día 23/05/2024. Sin embargo, se observa que el mencionado documento no ha sido formalizado o presentado ante el Comité de Institucional de Gestión y Desempeño.

Dicha aprobación cobra relevancia dado que según los lineamientos del MINTIC en la guía de roles y responsabilidades una de las funciones del Comité es "Aprobación seguimiento a los planes, programas, proyectos, estrategias y **herramientas necesarias para la implementación** interna de las políticas de seguridad y privacidad de la información" (negrita fuera de texto).

Por último, al revisar el documento se observa que la única exclusión identificada es la relacionada con los controles del numeral 6.2.2. dominio Teletrabajo y como justificación menciona "La entidad no ha establecido las disposiciones necesarias para dar cumplimiento a una política de teletrabajo, ya que no cuenta con los recursos pertinentes para implementar los requerimientos o directrices que se establece en la Ley 1221 de 2008 (Decreto reglamentario 0884 de 2012)".

Sin embargo, el documento de Política de Seguridad aprobado por la entidad se establece en el numeral 5.3.2. "*Teletrabajo o trabajo en casa Cuando se requiera realizar labores de teletrabajo el jefe del área y/o dependencia a la cual pertenece el servidor o contratista, debe solicitar a la Oficina de Gestión Tecnológica e Innovación la configuración de una VPN petición a mesadeservicio@loteriadebogota.com, los servicios, ambientes y aplicativos a los cuales se requiere acceder. El servidor o contratista se debe comprometer a hacer un uso adecuado de la VPN.*
En los casos en los cuales el acceso y procesamiento de la información de la LOTERÍA DE BOGOTÁ, sea mediante la modalidad de teletrabajo, los responsables de estas

Recomendación 6
Tema: Formalización de la Declaración de Aplicabilidad

Revisar y ajustar la declaración de aplicabilidad frente a otros documentos aprobados por la entidad.

Presentar ante el Comité Institucional de Gestión y Desempeño la Declaración de Aplicabilidad para su aprobación e implementación.

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

actividades deben dar cumplimiento a las condiciones y restricciones definidas entorno a la seguridad de la información, tales como: ➢ *Seguridad física.* ➢ *Acceso no autorizado a información o recursos*." Lo anterior evidencia debilidades en la definición de la Declaración de aplicabilidad.	
Observación 5 **Tema: Contexto Institucional** El día 22/05/2024 se recibe por parte de la Oficina de Planeación la matriz de contexto Institucional y revisado el documento se observa que si bien la Dirección de Operaciones identificó debilidades y amenazas cuya calificación es superior a 3, no definió las respectivas estrategias de tratamiento. Por otra parte, si bien es cierto en correo del día 27/05/2024 el jefe de la Oficina de Planeación informó que cuando finalice el primer semestre de la vigencia 2024 se realizará el respectivo seguimiento a las estrategias, la entidad no cuenta con este lineamiento documentado, lo que puede ocasionar que ante un cambio en la entidad o en los profesionales responsables del seguimiento, se pierda esta trazabilidad. La observación se socializó con la Oficina de Planeación el día 03/07/2024, a través de correo electrónico.	**Tema: Contexto Institucional** **Recomendación 7** Definir las estrategias para los factores con calificación de criticidad igual o mayor a 3. Dichas estrategias tienen como objetivo mitigar la amenaza (control), fortalecer la debilidad (acción de mejora), aprovechar las oportunidades, o mantener las fortalezas. **Recomendación 8** Documentar el lineamiento relacionado con el seguimiento periódico a las estrategias resultado del análisis del contexto institucional.
Observación 6 **Tema: Resolución 22 de 2011** El día 20/05/2024 se recibió de la Oficina de Tecnologías de la Información la Resolución 22 de 2011, la cual atiende a la pregunta asociada con la remisión del Acto Administrativo donde se adoptó en la entidad la Política de Seguridad de la Información. Si bien es cierto como se describe en la Conformidad No. 1 la entidad aprobó el MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN, en Comité Institucional de Gestión y Desempeño el día 16/08/2023, tal y como consta en el numeral 8 del acta de dicha sesión, la cual es el acto administrativo vigente para dicha política, revisando la Resolución 22 de 2011 se observa que la misma no está derogada y contiene aspectos que para este momento no están vigentes tales como: 1. Cita el Comité de Sistemas de Seguridad de la Información, el cual fue ingresado al Comité de Gestión Institucional de Desempeño	**Recomendación 9** **Tema: Resolución 22 de 2011** Revisar y actualizar de manera integral la Resolución 22 de 2011

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

2. La política definida en el artículo 14 está solo dirigida a funcionarios, ahora aplica para contratistas y partes interesadas 3. Cita a la dependencia como Oficina de Sistemas la cual cambio de denominación 4. Menciona formatos que no están vigentes como FRO202-153-1 5. Define horarios para acceder a los correos personales, ahora los permisos dependen de la configuración de privilegios del directorio activo 6. Define contraseñas de seis (6) caracteres, en la política vigentes son ocho (8) caracteres	
Observación No. 7 **Tema: Información de recursos asignados para la implementación del Modelo de Seguridad de la Información** Al realizar el análisis de la conformidad No. 5 se observó que la entidad no tiene consolidada la información sobre los recursos que asigna a la adopción, implementación, mantenimiento y mejora continua del MSPI. Esto dado que dichos recursos son financieros, humanos (dedicación de horas/hombre) de sus colaboradores y en general cualquier recurso asignado de manera transversal; es decir, no son únicamente los recursos de la Oficina de Tecnologías de la Información, sino que es posible que se asignen recursos que contribuyan al modelo pero sean administrados o supervisados por otras dependencias. Esta observación se basa en el hecho que el día 27/05/2024 se realizó mesa de trabajo con la Oficina de Planeación quienes manifestaron no tener la información de recursos asignados al MSPI, por lo tanto, se envió el requerimiento No. 8 dirigido a la Secretaría General, el jefe de la Oficina de Tecnologías de la Información y el Jefe de la Unidad Financiera. El día 04/06/2024 se recibe respuesta del Jefe de la Unidad Financiera quien manifiesta “Desde la Unidad Financiera y Contable no es posible saber qué fue lo que proyectó el área de sistemas en el presupuesto 2023 y 2024 para el MSPI. El profesional responsable del área debe indicar que recursos determinó para ser ejecutados en el presupuesto 2023 y cuales en el presupuesto 2024. Con esa información desde la Unidad Financiera podríamos confirmar que dichos recursos se encuentran, ejecutados para la vigencia 2023, y apropiados o ya ejecutados para la vigencia 2024”.	**Recomendación 10** **Tema: Información de recursos asignados para la implementación del Modelo de Seguridad de la Información** Determinar el área responsable de consolidar la información sobre los recursos que la entidad asigne para la adopción, implementación, mantenimiento y mejora continua del MSPI

FIRMA DEL INFORME DE AUDITORÍA:

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

FECHA DE APROBACIÓN:		
NOMBRE	**RESPONSABILIDAD**	**FIRMA**
Wellfin Jhonathan Canro Rodríguez	Jefe Oficina de Control Interno	
Luz Dary Amaya Peña	Auditora líder	
No aplica	Auditor Acompañante	

Documento Maestro *Modelo de Seguridad y Privacidad de la Información MSPI*, expedido en octubre de 2021. Link. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf