ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE AMBIENTE

SECRETARÍA DISTRITAL DE AMBIENTE **Folios**: 20. **Anexos**: No.
Radicación #: 2019IE301972 **Proc** 4671764 **Fecha**: 2019-12-26 09:41
Tercero: 899999061-9 126 - SECRETARIA DISTRITAL DE AMBIENTE
Dep Radicadora: JEFE OFICINA DE CONTROL INTERNOClase Doc:
Interno **Tipo Doc**: Memorando **Consec**:

MEMORANDO

PARA: **ROSANNA SANFELIU GIAIMO**
Directora de Planeación y Sistemas de Información Ambiental

MARIA MARGARITA PALACIO RAMOS
Directora de Gestión Corporativa

OSCAR FERNEY LÓPEZ ESPITIA
Subsecretario General y de Control Disciplinario

DE: **SANDRA ESPERANZA VILLAMIL MUÑOZ**
Jefe oficina de Control Interno

ASUNTO: Alcance informe de seguimiento especial estrategia de gobierno digital Decreto 2573 de 2014 y Ley de transparencia y del derecho de acceso a la información pública Ley 1712 de 2014.

Reciban un cordial saludo.

La Oficina de Control Interno en cumplimiento del plan anual de auditorías 2019 comunicó mediante forest No. 2019IE278817 del 30 de noviembre de 2019, los resultados del seguimiento especial a la implementación *Ley de Transparencia y del Derecho de Acceso a la Información Pública Ley 1712 de 2014,* mediante el presente documento se presenta los resultados de la verificación de la adopción de los requisitos del Decreto 2573 de 2014 y de la norma ISO 27001:2013, en los siguientes términos:

Objetivo:

Realizar seguimiento la implementación los controles de la norma NTC ISO 27001:2013 y los requisitos establecidos en el Decreto 2573 de 2014 en el marco de las políticas de gobierno digital y política de seguridad de la información, como parte de la dimensión 3, gestión con valores para el resultado, del modelo integrado de Planeación y Gestión -MIPG.

Alcance:

Los controles de la norma NTC ISO 27001:2013 y los requisitos establecidos en el Decreto 2573 de 2014 durante las vigencias 2017, 2018 y 2019.

I. METODOLOGÍA

Análisis de la información remitida por la Dirección de Planeación y Sistemas de Información Ambiental -DPSIA mediante forest No. 2019IE261594 el 8 de noviembre de 2019, la información disponible en los sistemas de información forest, ISOlucion, página web de la SDA y la validación de la información mediante entrevistas con los responsables asignados por el proceso.

II. RESULTADOS

El proceso ha definido para revisar el avance en la implementación del SGSI las siguientes herramientas:

a. Indicador en ISOlucion "Avance en la implementación de los controles de la NTC-ISO 27001:2013, en la Secretaría Distrital de Ambiente"

Presenta seguimientos trimestrales con resultados del 100% para la meta: Avanzar a 31 de diciembre de 2019 en diecisiete (17) controles, durante el año 2018 se avanzó en (11) y en el 2017 se avanzó en (28) controles, para un total de 56 controles., al respecto se encontró que:

Vigencia	Situación Observada
2017	El resultado del indicador código 750 en ISOlucion con corte 31 de diciembre de 2017 registra como implementados (28) controles, según documento disponible en el sistema de información *"Plan de trabajo"* para la implementación SGSI se relacionan 28 ítems que al compararlos con los controles de la norma NTC-ISO 27001:2013 sólo se logra identificar (20) controles, siendo complejo verificar a que número de control específico se asoció para su implementación, dado que: a). Los ítems del No. 19 al No. 28 sólo se relacionan procedimientos a implementar, por ejemplo: Política procedimiento de uso adecuado de internet, procedimiento de no repudio, procedimiento de criptografía y gestión de llaves, entre otros. b). En los ítems: el No. 3 hace referencia al subgrupo A.14.2, el No. 7 hace referencia al subgrupo A.7.2 y el No. 12 hace referencia al subgrupo A.8.3, al reportar por subgrupos no permite evidenciar a cuál o cuáles controles son los que realmente fueron reportados como implementados, es importante señalar que sólo en estos tres subgrupos incluyen 28 controles. c). Los ítems números 7, 8, 13, 15, 16 y 18 no registran cumplimiento del control.

Vigencia	Situación Observada
2018	El resultado del indicador código 750 en ISOlucion con corte 31 de diciembre de 2018 registra como implementados (11) controles, según reporte del primer semestre se avanzó en 7 controles que corresponden a los números: A.8.2.1, A.8.2.3, A.9.1.1, A.7.2.2, A.7.1.2, A.6.2.1, A.13.1., para el segundo semestre se avanzó en 6 controles correspondientes a los números A.9, A.18.1, A.15, A.8.1, A.12.6, A.16, siendo complejo verificar a que número de control específico se asoció para su implementación, dado que: a) Reportar por grupos como el A.9, A.15 y A.16 que incorporan más de un control, genera incertidumbre en el reporte del indicador. b) Reportar por subgrupos como el A.18.1, A.8.1 y A.12.6 que incorporan más de un control, genera incertidumbre en el reporte del indicador. c) En total de grupos y subgrupos reportados, suman 37 controles.
2019	El resultado del indicador código 750 en ISOlucion con corte 30 de junio de 2019 registra como implementados (08) controles con números A.8.2.1, A.8.2.3, A.9.1.1, A.12.6, A13.1, A13.1.2 A.12.2 y A.17.1, quedando para el segundo semestre (9) controles a reportar, se observa que: Igual como se mencionó para la vigencia anterior, reportar controles como subgrupos A.12.6, A13.1, A.12.2 y A.17.1 genera incertidumbre en el reporte del cumplimiento, dado que los anteriores subgrupos contienen un total de 12 controles.

Además, se observa que:

a). Los controles números A.8.2.1 y A.9.1.1, fueron reportados como implementadas en las vigencias 2017, 2018 y 2019.
b). El control No. A.8.2.3, y subgrupo A.13.1, fueron reportados en las vigencias 2018 y 2019.
c). Los controles A.7.1.2 y A.6.2.1 fueron reportados en las vigencias 2017 y 2018

Lo anterior podría sobredimensionar el reporte de cumplimiento del indicador, se observa que los controles reportados como cumplidos no guardan relación con los reportes de la meta establecida *"56 controles a implementar a 31-12-2019"*.

A manera de ejemplo para los controles reportados en más de una vigencia, se observa que en los seguimientos a los controles A.8.2.1 y A.8.2.3 *"Clasificación de la información"*, el proceso informa en la vigencia 2019: *"…, se está llevando a cabo la Actualización de los activos de información y la revisión de los riesgos de seguridad de la información"*, en el 2018 *"…mediante la actualización del cuadro de caracterización, su instructivo de diligenciamiento y el ajuste del procedimiento 126PA06-PR02 que lo contiene, desarrollado en conjunto entre el grupo SIG y las dependencias de la entidad, incluyendo la clasificación en función de los requisitos legales y el enfoque de seguridad de la información",* en el 2017 "*Información Clasificada en Función de requisitos legales, valor, criticidad y*

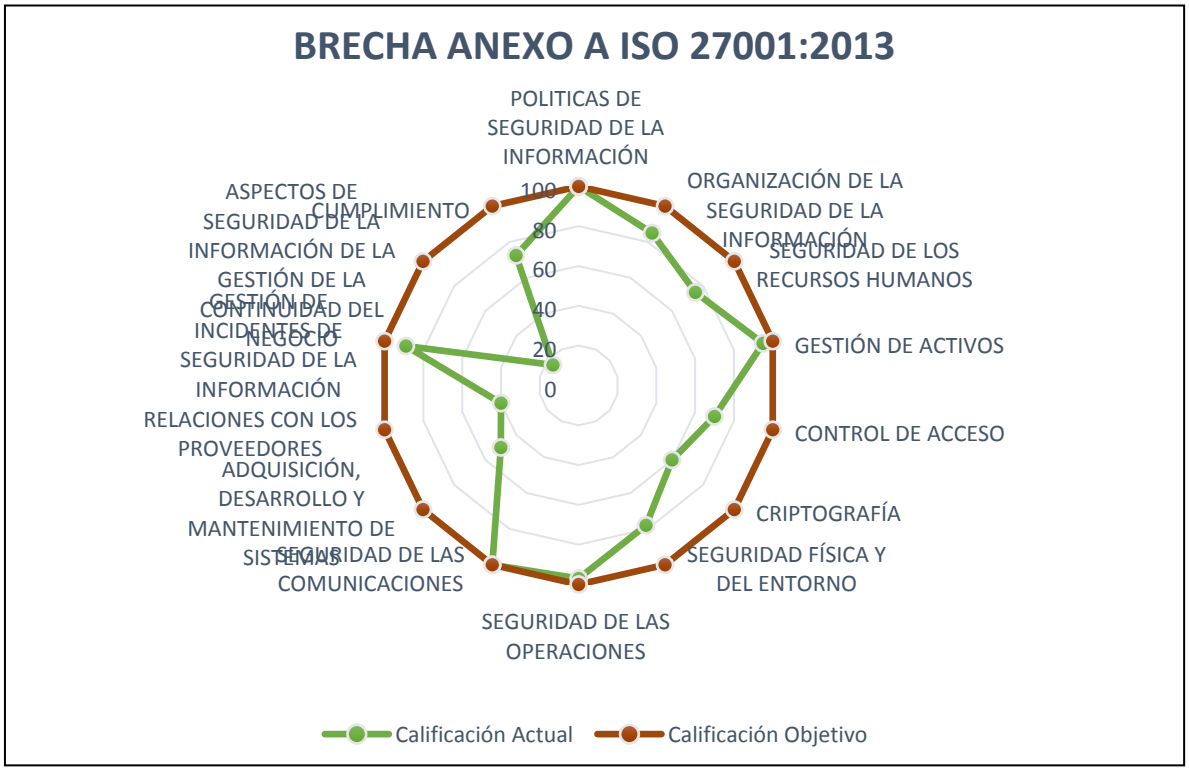
susceptibilidades", información que solo corresponde a avances en la implementación del grupo A.8 "Gestión de recursos" conformado por tres (03) subgrupos y 10 controles.

Por otro lado, verificando con el proceso se evidenciaron avances en el ajuste del inventario de activos, lo que significa que se estaría avanzado en el control A.8.1.1 Inventario de Activos y el A.8.1.2 propiedad de los activos, los cuales en los seguimientos en ISOlucion no reporta avances sobre estos.

Por último, de acuerdo con las evidencias aportadas, se observa que en el Manual del subsistema de gestión de la seguridad de la información (SGSPI) 126MSGSI Versión: 1.0 en el ítem 7.3 indicadores y medición de la seguridad de la información, se observa que para la meta del año 2018 se estableció implementar los 114 controles de la norma ISO 27001:2013 lo cual no concuerda con la meta definidos del indicador de gestión a 31-12-2019 implementar 56 controles, información reportada en la revisión por la dirección del mes de noviembre de 2019 con los 56 controles implementados.

b. Instrumento de identificación línea base de seguridad de Modelo de Seguridad y Privacidad de la Información -MSPI.

Se observa que en el aplicativo ISOlucion se encuentra el instrumento de evaluación del MSPI – SDA en el cual presenta en el cuadro de "evaluación de efectividad de controles" una calificación actual de 62 puntos (diagnóstico a 2017) y en la herramienta remitida actualizada julio 2019" tiene una calificación de 73 puntos, de lo cual es importante mencionar que para el grupo A.10 no se ha priorizado, y para los grupos A.14, A.15 y A.17, a pesar de los reportes de implementación presentan menores avances tal como se muestra en la siguiente grafica "Brechas anexo A ISO 27001:2013".



Fuente DPSIA diciembre de 2019

c. Documento "Declaración de aplicabilidad"

Se observa que fueron excluidos tres (03) controles de los 114 controles que especifica el Anexo A de la norma ISO 27001:2013, donde se especifica la justificación de las inclusiones más no la justificación para las exclusiones, por lo que no se cumple con el numeral 6.1.3 tratamiento de riesgos de la seguridad de la información literal d) que menciona *"Producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c) y la justificación de las inclusiones, ya sea que se implemente o no* ***y las justificaciones para la exclusiones de los controles A****." Negrilla fuera de texto.*

Al revisar el contenido del documento "Declaración de aplicabilidad" publicada en ISOlucion, se observa que registra 11 controles cumplen satisfactoriamente, 25 no cumplen y 78 cumplen parcialmente, información que no guarda relación con la reportada en la revisión por la dirección de noviembre de 2019, en la cual reporta la implementación de 56 controles de la meta propuesta.

d. Documento "Pruebas de efectividad del SGSI de la SDA"

No se logró evidenciar los ejercicios de pruebas de efectividad ni los registros en el plan de mejoramiento de las vulnerabilidades y amenazas que permitan evidenciar lo indicado en la Guía Metodológica de Pruebas de Efectividad versión del 06/05/2016 del MINTIC, que permita identificar las brechas frente a la norma ISO 27001 y los requisitos frente al MSPI.

e. Plan Estratégico de Tecnología de Información -PETI

En el PETI se definieron cuatro (04) indicadores, para los cuales tres (03) cuenta con reporte de seguimiento corte 30-06-2019 y los resultados se enuncian a continuación:

- Código 1008 - Cumplimiento de las fases de proyectos del PETI

  Según reporte de seguimiento en ISOlucion primer semestre 2019 el resultado es de 69% para la meta *"A 31 de diciembre de 2019 alcanzar el 100% de cumplimiento en las fases de proyectos del PETI"*

- Código 1009 - Cumplimiento presupuestal de los proyectos del PETI

  Según reporte de seguimiento en ISOlucion primer semestre de 2019 el resultado es de 41% para la meta *"A 31 de diciembre de 2019 alcanzar el 100% de cumplimiento presupuestal de los proyectos del PETI"*

- Código 1007 - Porcentaje de proyectos PETI al día en cronograma (código 1007)

  Según reporte de seguimiento en ISOlucion primer semestre de 2019 el resultado es de 69% para la meta *"A 31 de diciembre de 2019 alcanzar el 90% de proyectos PETI al día en cronograma"*

- Código 1006 - Porcentaje de ejecución y cumplimiento de los programas – Proyecto definidos en toda la vigencia del PETI

  En la matriz de seguimiento de indicadores, se observa un reporte parcial con resultado del 50%.

El PETI v3 actualizado definió 17 proyectos identificados con los números P1, P2, P3, P7, P8, P9, P10, P11, P13, P14, P15, P18, P22, P23, P32, P24 y P26 a implementar (ver siguiente tabla), en estos se incluyen fichas donde se detallan de acuerdo con unas fases (iteracciones), actividades, tareas y entregables Anexo 1, al revisar los resultados del seguimiento corte 30 de junio de 2019 remitido mediante forest No. 2019IE290257 del 13 de diciembre de 2019, se observa que:

PROYECTO	# Fases Completadas	# Fases Planeadas	CPE= Cumplimiento de proyectos entregados
P1. Definición e implementación de la estrategia de TI para la SDA	3	3	100%
P2. Definición e implementación del proceso formal de arquitectura empresarial para la SDA	1	2	50%
P3. Definición, actualización e implementación de procedimientos de TI basados en las mejores prácticas de ITIL	1,5	2	75%
P32. Institucionalización y apropiación de los lineamientos y mejores prácticas del Dominio de Uso y Apropiación.	2	2	100%
P9. Diseño e implementación de datos maestros	0	3	0%
P10. Diseño e implementación del modelo de Gobierno de Información	0	3	0%
P7. Diseño e Implementación de Inteligencia de Negocios	0	5	0%
P8. Fortalecer y formalizar el modelo de gestión de Datos Abiertos	2	3	67%
P22. Diseño e implementación del modelo de interoperabilidad	0	5	0%
P23. Diseño e implementación de Reglas de negocio y	3	4	75%
P24. Diseño e implementación del modelo de gestión documental	3	3	100%
P26. Implementación del sistema de gestión de identidades	0	0	Declarado Inviable
P11. Análisis, diseño e Implementación del BIA (Análisis de Impacto al Negocio), DRP (Plan de Recuperación de Desastres) y BCP (Plan de Continuidad del Negocio)	0	4	0%
P13 Análisis, Diseño e Implementación de un plan de Capacidad	1	2	50%
P14 Análisis, Diseño e Implementación de un plan de Mantenimiento consolidado de la infraestructura tecnológica que soporta la SDA.	2,75	3	92%
P15 Análisis, Diseño e Implementación de un plan de pruebas de Backup y restauración	1,8	3	60%
P18. Gestión del Modelo de Seguridad y Privacidad de Información	3	4	75%

Fuente DPSIA diciembre de 2019

a) El proyecto P26 fue declarado como inviable.
b) En el proyecto P18 fueron programas 6 fases, pero no fueron definidas actividades ni entregables.
c) Los proyectos P7, P9, P10, P11, P14 y P22 de acuerdo con el reporte de seguimiento indicadores ISOlucion del 30 de junio de 2019, informa que está pendiente determinar su priorización y su asignación presupuestal para definir si se realizará alguna ejecución en la vigencia 2019 para las fases (iteraciones) relacionadas en el PETI V3 donde sí se relaciona recursos.
d) El resultado del indicador 1007 reporta cumplimiento de 9 proyectos, identificados con los números P1, P2, P3, P32, P8, P23, P24, P13, P15 y P18; y en el registro de seguimiento a indicadores PETI, indica avance de los anteriores proyectos y adiciona reporte para el proyecto P2.
e) El resultado del indicador 1008, reporta cumplimiento de 10 proyectos identificados con los números P1, P2, P3, P32, P8, P23, P24, P13, P15 y P18; y en el registro de seguimiento a indicadores PETI reporta avance para el proyecto P14.

f) Con respecto al proyecto P1, reporta 100% de cumplimiento pero para la actividad 3 *"Ajuste políticas y estándares de TI"* no se logra evidenciar su cumplimiento. Además, se observa en el PETI v3 programación de recursos en la vigencia 2020 por valor $94 millones y no hay fase o actividades programadas.
g) Con respecto al proyecto P2, se observa en el PETI v3 programación recursos para la vigencia 2020 por valor $138 millones pero no hay fases ni actividades programadas.
h) Con respecto al proyecto P3 se observa en el PETI v3 se han programado tres fases (iteraciones) y tres actividades, una para cada vigencia 2018, 2019 y 2020, en cuadro de seguimiento del indicador PETI se registran solo dos fases programadas. Por otro lado, se observa que aún no han sido aprobado los procedimientos para gestión de problemas y gestión de cambios implementados y para la gestión de eventos, gestión de catálogo de servicios de TI , gestión de proveedores, backups, definidos para el 2019, siendo que la fase fue reportada como cumplida.
i) Con respecto a los proyectos P9 y P10, se observa en el PETI v3 programación de fases (iteraciones) y sus actividades para el 2019 y para 2020, pero en el cuadro de seguimiento indicador se registran las tres fases programadas para el 2020.
j) Con respecto a los proyecto P7, se observa en el informe de seguimiento PETI que no se reporta avance siendo que el PETI se encuentra actividad y fase programada en el 2019, en el seguimiento indicadores PETI se programan las 5 fase para el 2020 y ninguna para el 2019.
k) Con respecto al proyecto P8, se observa que fueron reportadas como cumplidas las dos fases programadas, sin embargo el entregable "Inventario de activos de información de la Entidad con la respectiva categorización para ser publicado como Datos abierto" se evidenciaron avances, pero aún no ha sido publicados en los sistemas de información de la entidad.
l) Con respecto al proyecto P18, se observa en el PETI v3 programación de cuatro fases, una para la vigencia 2019, en el registro de seguimiento del indicador PETI para la fase 3 programada en la vigencia 2019 se reporta cumplida, pero no se logró evidenciar cumplimiento de la actividad *"Diseño e implementación del plan de mejora continua del SGSI"*

De lo anterior, se observa que la información reportada presenta inconsistencias, situación que con lleva a no tener certeza el grado de avance del PETI, lo que podría dificultar la toma de decisiones y la identificación de brechas a cerrar para su implementación.

No obstante lo anterior, los responsables del proceso desde el mes de agosto de 2019, ha implementado como medida de corrección dos estrategias: la primera identificar en las gerencias de los proyectos de inversión profesionales de enlace con los cuales se puede tener comunicación directa que permita determinar y validar en las actividades en las necesidades de contratación los componentes de

tecnología de información -TI y la segunda está relacionada con la definición de un procedimiento mediante el cual todas las gerencias de proyectos informen y trabajen de forma armónica la identificación de los componentes de TI para las actividades a contratar.

Recomendaciones:

- Revisar las diferentes herramientas o instrumentos de planeación y evaluación del SGSI *"Reporte indicador gestión ISOlucion", "Instrumento de identificación línea base de seguridad de Modelo de Seguridad y Privacidad de la Información –MSPI" y "Declaración de aplicabilidad"* con el fin de que estos se actualicen de forma armónica, que faciliten validar la información de la primera y segunda línea de defensa y poder así identificar las brechas para alcanzar los resultados esperados.
- Actualizar el PETI y definir un plan de trabajo anual que incluya los 16 proyectos con el nivel de detalle de las actividades, tareas o entregables, se establezca línea base y facilite confrontar la programación con respecto a las actividades desarrolladas.
- Revisar los reportes de seguimiento del PETI *"reporte indicadores de gestión ISOlucion", "Informe primer semestre 2019 PETI" y "matriz de seguimiento indicadores PETI"* con el fin de que la información guarde relación entre estas, que faciliten validar la información primera y segunda línea de defensa y poder así identificar las brechas para alcanzar los resultados esperados.
- Elaborar plan de mejoramiento las vulnerabilidades y amenazas detectadas en las pruebas de efectividad SGSI de la SDA como se menciona en el numeral 4 del documento Pruebas de efectividad *"Se debe registrar en el plan de mejoramiento las vulnerabilidades y amenazas detectadas en cada una de las pruebas, la causa raíz, las acciones correctivas o de mejora que apliquen, los responsables y las fechas de ejecución de cada acción; todo esto siguiendo el procedimiento de Plan de mejoramiento por Procesos con el que cuenta la entidad referente al SIG"*
- Agilizar la definición del procedimiento identificación de los componentes de TI para las actividades a contratar y la aplicación de la herramienta de armonización del PETI y PAA, que permita identificar la totalidad de los contratos a realizar por parte de las áreas a cargo de los proyectos de inversión números 1141, 978, 979, 981 y 1100 a suscribir en la vigencia 2020.

1. IMPLEMENTACIÓN SGSI

El proceso para la implementación de sistema de gestión de seguridad de la información tomo como base los controles definidos en la norma ISO/IEC 27001:2013.

CONTROLES ANEXO A	DESCRIPCION DEL DOMINIO

No.	Código Dominio	Cantidad de Controles	
1	A.5	2	Políticas de seguridad de la información
2	A.6	7	Organización de la seguridad de la información
3	A.7	6	Seguridad de los recursos humanos
4	A.8	10	Gestión de activos
5	A.9	14	Control de acceso
6	A.10	2	Criptografía
7	A.11	15	Seguridad física y del entorno
8	A.12	14	Seguridad de las operaciones
9	A.13	7	Seguridad de las comunicaciones
10	A.14	13	Adquisición, desarrollo y mantenimiento de sistemas
11	A.15	5	Relaciones con los proveedores
12	A.16	7	Gestión de incidentes de seguridad de la información
13	A.17	4	Aspectos de seguridad de la información de la gestión de la continuidad del negocio
14	A.18	8	Cumplimiento

1.1 Políticas de Seguridad de la Información (A.5)

Situación Observada: Se evidencia que el documento políticas de seguridad de la información publicado en ISOlucion no ha sido revisado desde el año 2017 y desde esta fecha se han promulgado nuevas normas al respecto como el Decreto 1008 del 2018 por el cual se establecen los lineamientos generales de la política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión que establece en la dimensión Gestión con Valores para el Resultado, política de Gobierno Digital. El Control A 5.1.1 indica que las políticas para la seguridad de la Información se deben revisar a intervalos planificados, o si ocurren cambios significativos.

Al revisar el contenido de las políticas definidas con respecto a lo indicado en el documento Guía 2 - Política General MSPI v1, se observa lo siguiente:

1). La política de organización de la seguridad de la información de la entidad hace referencia al comité del Sistema Integrado de Gestión el cual fue reemplazado por el Comité institucional de gestión y desempeño creado mediante Resolución SDA 915 de 2019.

2) La Política de activos de información no determina la periodicidad con la cual se va a realizar al interior de la Entidad la identificación y/o actualización del inventario de Activos de Información, como lo indica el ítem 9.2 de la Guía 2 - Política General MSPI v1.

4). La Política de No repudio no considera temas, como: retención y trazabilidad y menciona procedimientos que no están formulados, como: No-repudio de Origen y el No-repudio de Recepción, de acuerdo con lo indicado el ítem 9.4 de la Guía 2 - Política General MSPI v1.

5). La Política Privacidad no abarca todos los principios del tratamiento de datos personales como el de la Legalidad y Libertad. Por otra parte, en cuanto a la Política de Confidencialidad no se establece cuando se firma el acuerdo de confidencialidad, así como la vigencia de este, como lo indica el ítem 9.5 de la Guía 2 - Política General MSPI v1.

Recomendaciones:

- Asegurar que Políticas del SGSI se revisen a intervalos planificados, con el fin garantizar la conveniencia, adecuación y eficacia y se armonice con la Política de Gobierno Digital, Manual de Gobierno Digital Implementación de la política digital de acuerdo con lo señalado en el Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2).
- Considerar la inclusión y/o actualización de los parámetros que indica en cada una de las Políticas específicas para la implementación de controles de seguridad de la información indicadas en la Guía 2 - Política General MSPI v1 del 11/05/2016.

1.2 Organización de la Seguridad de la Información (A.6)

Situación Observada: En cumplimiento con el control A.6.1.1 se revisa el manual SGSI código 126MSGSI ítem 3.2 Roles y Responsabilidades de la Implementación del Plan de sensibilización del SGSI y en el documento en ISOlucion *"Roles responsabilidades y autoridades para el SGSI de la Secretaria Distrital de Ambiente – SDA"* donde se definen y asignan las responsabilidades para la seguridad de la información a los responsables asignados de las Direcciones de Planeación y Sistemas de Información -DPSIA y las Dirección de Gestión Corporativa –DGC,

No obstante, lo indicado en el Decreto 109 de 2009 estructura organizacional de la SDA en los artículos 13 y 25, señalan responsabilidades relacionadas con la administración de los recursos informáticos y la organización del sistema de información ambiental, se observa que para la implementación del SGSI no fueron definidas autoridades para la DGC y ni responsabilidades a las áreas misionales que administran recursos TI, puesto que estas áreas administran recursos y canalizan necesidades de tecnologías de información en especial para los proyectos de inversión (1141, 978, 979, 981) y los rubros de funcionamiento, situación que facilitara dinamizar gobernanza del SGSI.

Para los controles A.6.1.3 y A.6.1.4 se mantiene contacto con las autoridades y grupos de interés especial con el Ministerio de las Telecomunicaciones (MINTIC) y la Alta Consejería de las TIC (ACDTIC) y para los controles A.6.2.1 y A.6.2.2 están documentadas las *Políticas de Dispositivos Móviles y Teletrabajo* en las políticas de Subsistema de Gestión de

Seguridad de la Información y se encuentra los procedimientos de 126PA03-PR13 "Gestión de incidentes y requerimientos", 126PG02-PR01 "Comunicación Externa", 126PG02-PR02 *"Comunicación Interna"* donde se establecen las especificaciones de cuándo y a través de a quien se debería contactar a las autoridades. Se observa el Directorio de contacto para seguridad de la información de la SDA donde se evidencia el cumplimiento del control A.6.1.3 y A.6.1.4.

Por otro lado, no se pudo evidenciar que para SGSI se haya establecido un alcance que contemple todos los recursos disponibles que tiene la entidad para la seguridad de la información, como, por ejemplo, contemplar aquella información contenida en los equipos de tecnológicos asignados a los funcionarios autorizados para realizar teletrabajo.

Recomendaciones:

- Evaluar la pertinencia de actualizar el documento de *"Roles responsabilidades y autoridades en la SDA para el subsistema de gestión de seguridad de la información– SGSI de la Secretaria Distrital de Ambiente – SDA"* considerando lo indicado en el numeral 6.3.2 de la guía N°4 Roles y responsabilidades de MINTIC del 25/04/2016 que menciona *"Teniendo en cuenta la naturaleza de la entidad, debe conformarse un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente".* Entre los posibles perfiles podrían estar un representante del área Jurídica.
- Establecer el alcance del SGSI donde se determine los límites y la aplicabilidad teniendo en cuenta las cuestiones externas e internas, las partes interesadas, las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones de acuerdo con el numeral 4.3 de la ISO 27001 de 2013. Además, el alcance debe estar disponible como información documentada.

1.3 Seguridad de los Recursos Humanos (A.7)

Situación Observada: Se encuentra que el manual del SGSI 126MSGSI en el ítem 3.2 Roles y Responsabilidades de la Implementación del Plan de sensibilización del SGSI, se observó documento en ISOlucion "Roles responsabilidades y autoridades para el SGSI – SDA. De los documentos aportados se encuentra: Acta y registro del 23 de agosto de 2019 de sensibilizaciones del SGSI, a los contratistas y funcionarios de la Subdirección de Silvicultura, Flora y Fauna Silvestre; también el Formato de cláusulas comunes a los contratos de prestación de servicios profesionales y de apoyo a la gestión: En las obligaciones generales del contratista se establecen obligaciones en materia de seguridad de información, numerales 3, 4, 6, 7,12, Contratos números SDA–CPS- 20190364, SDA–CPS- 20190520, SDA–CPS- 20190520, SDA–CPS- 20190562 y el Plan de Sensibilización del SGSI de la SDA 2019 y las Políticas del SGSI.

Se observa que el documento de Ingeniera Social, vigencia 2019, sin fecha de aprobación, se encuentra revisado y aprobado por dos profesionales del proceso, el cual debería ser aprobado por el líder del proceso.

Recomendaciones

- Asegurar que las sensibilizaciones y capacitaciones programadas en el Plan de Sensibilización del SGSI de la SDA incluyan los resultados de los ejercicios de Ingeniera Social, participe todo el personal que labora en la entidad.
- Sensibilizar a los funcionarios en buenas prácticas de seguridad de la información, en el uso responsable de USB, el no suministro de credenciales personales, el cambio periódico de contraseñas y la no configuración de recordar credenciales.
- Garantizar que todo el personal de la SDA tenga conciencia de la pertinencia e importancia de sus actividades en la seguridad de la información y cómo ellas contribuyen al logro de los objetivos del SGSI, con el fin de dar cumplimiento al numeral 5.2.2 Formación, toma de conciencia y competencia de la ISO/IEC 27001:2013.
- Garantizar que la aprobación de los documentos como el informe de ingeniera social sean aprobados por los Directivos responsables del proceso y sean socializados a toda la entidad.

1.4 Gestión Activos (A.8)

Situación Observada: Se ha avanzado en la implementación de los 10 controles en temas relacionados con el dominio de Gestión de activos, evidenciándolo en el procedimiento PA06-PR02 Administración y control de los activos y registros de información y se consolida parcialmente la matriz de activos de información de la entidad, que se encuentra en elaboración con las dependencias de la entidad.

Recomendaciones:

- Finalizar con la consolidación del *PA06-PR02-F1 Inventario de activos de información no documental* de la entidad conforme al procedimiento *PA06-PR02 Administración y control de los activos y registros de información,* que permita asegurar los criterios de disponibilidad, integridad y confidencialidad. *Además,* incorporar en el Inventario el control de cambios que asegure su trazabilidad.
- Asegurar que se documenten "*las reglas para el uso aceptable de información y activos asociados con la información e instalaciones del procesamiento de la información"*, en cumplimiento del control A.8.1.3 de la ISO 27001:2013.

1.5 Control de Acceso (A.9)

Situación Observada: En el numeral 3 Control de Acceso de las Políticas del SGSI v1, se establecen las responsabilidades de la DPSIA y los usuarios, se evidencia que al momento del retiro del personal se realiza ajuste de los derechos de acceso a usuarios por terminación o cambio de funciones.

Por otra parte, se observa que no se ha documentado la aplicación de los subgrupos A.9.2 y A.9.3 referentes a la gestión de acceso de usuarios y uso de la información de autenticación secreta, las revisiones de los derechos de acceso a intervalos regulares y el Uso de información de autenticación secreta.

Recomendación:

Documentar los controles que se llevan a cabo para la asignación de información de autenticación secreta conforme al control A.9.2.4. Las revisiones y cobertura de los derechos de acceso de los usuarios, las cuales deben realizar a intervalos regulares conforme a lo establecido en el control A.9.2.5 y el uso de información de autenticación secreta para el control A.9.3.1.

1.6 Criptografía (A.10)

Situación Observada: Las Políticas del SGSI Vi mencionan en el numeral 7 la política de criptografía y gestión de llaves, no se logró evidenciar herramientas y/o registros para su aplicación.

Recomendación:

Fortalecer la implementación del control A.10.1.2 respecto a la gestión de llaves donde se garanticen que se proteja el tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida, de conformidad con lo establecido en la Guía procedimientos de seguridad de la información v1 del 25/04/2016 numeral 6.4 Criptografía, procedimientos para controles criptográficos y gestión de llaves criptográficas.

1.7 Seguridad Física y del Entorno (A.11)

Situación Observada: Se encuentra la Directiva 003 del 24 de febrero se establece la política de Escritorio limpio y Pantalla Limpia y se evidencia su respectiva socialización.

Revisado el seguimiento del indicador Indicador ISOlucion *"Avance en la implementación de los controles de la NTC-ISO 27001:2013, en la Secretaría Distrital de Ambiente" de la vigencia 2017,* se implementaron 28 controles según matriz de "Priorización de los controles a implementar - sistema de gestión de la seguridad de la información SGSI, anexo A ISO 27001:2013", se observa que se reportó como implementado los controles A11.1.5 establecimiento de criterios para trabajos en áreas seguras y seguridad física y ambiental,

A11.2.8 directrices para la protección de equipos desatendidos y A11.2.7 proceso de borrado de discos y de encriptación del disco, los cuales no se encuentran disponibles para su uso en el ISOlucion.

Recomendación

Documentar las actividades para asegurar el cumplimiento de los controles A11.1.5, A112.7 y A11.2.8 que permitan definir los criterios para; a) trabajos en áreas seguras, b) seguridad física y ambiental, c) protección de equipos desatendidos y d) borrado de discos y de encriptación del disco.

1.8 Seguridad de las Operaciones (A.12)

Situación Observada: El 17 de junio de 2019 se presentó un incidente de Seguridad de la Información en la herramienta del Sistema de Información para el Recaudo de Visitas Técnicas "ONTRACK" de la Secretaria Distrital de Ambiente reportado por parte del proveedor externo mediante el PA03-PR14-M1 Valoración de eventos e incidentes de seguridad de la información.

Se realizó la prueba de Ingeniería Social donde se obtuvieron resultados claves para generar estrategias para fortalecer la cultura en seguridad de la información y se generó Informe de Seguridad Servidor RMCAB (vulnerabilidades) con fecha del junio 30 de 2019.

La entidad recientemente adquirió mediante contrato SDA-SI-2019400 el día 24 de octubre de 2019 el soporte y configuración de un antivirus endpoint protection de nueva generación, reemplazado la actualización del antivirus adquirida mediante proceso contractual SDA-MC-0182018 del 28 de junio de 2018, observando que los equipos de cómputo de la entidad estuvieron por un periodo de tiempo sin el antivirus, así mismo no se evidenciaron registros de acciones implementadas para mitigar los efectos adversos, situación asociada al riesgo implementado por el proceso denominado *"R2 Afectación de la confidencialidad, disponibilidad e integridad; y privacidad de la información"* de la cual no se ha documentado como posibles causas la afectación por virus y sus medidas de mitigación para su reducción.
Por otro lado, con respecto al riesgo implementado por el proceso "R1 Intermitencia o indisponibilidad de los servicios de tecnologías de la información y Comunicaciones", como posible causa se identificó *"No tener definido el plan de continuidad de negocio para TI, ni el plan de recuperación de desastres sobre de los servicios tecnológicos.."*" se observa que dichos planes no han sido definidos y no se establecieron en el mapa de riesgos acciones para reducir el riesgo.

De acuerdo con el reporte de fecha 12 de diciembre de 2019 del antivirus Bitdefender, se observa que 709 equipos que cuentan con actualización de antivirus de 930 de equipos con que cuenta la entidad, además a la fecha los equipos de cómputo asignados a los trabajadores en teletrabajo no se les actualizado el antivirus.

Recomendaciones:

- Socializar en las reuniones de autocontrol los resultados de los diferentes informes que se generen, documentando las acciones de mejora para el SGSI.
- Agilizar la instalación del nuevo licenciamiento del antivirus en la totalidad de los equipos de cómputo de la entidad.
- Revisar en el mapa de riesgos del proceso los riesgos R1 y R2 con el fin de que se establezcan acciones de mitigación relacionadas con: Definir e implementar plan de continuidad del negocio, plan de recuperación de desastres y seguimiento a la adquisición o renovación del licenciamiento del antivirus.

1.9 Seguridad de las comunicaciones (A.13)

Situación Observada: Para la gestión de seguridad en DataCenter y de las Redes, se realiza mediante la actualización del firmware que controla físicamente los dispositivos, la herramienta Q-Radar se gestiona los bloqueos en Firewall, el SANDBOX que detecta y encapsula varios Malwares con nivel Alto de ataque y propagación y se cuenta con herramientas como el NAGIOS y CACTI donde se monitorizan las redes que vigilan los equipos y servicios de la entidad.

1.10 Adquisición, desarrollo y mantenimiento de sistemas (A.14)

Situación Observada: Revisado el seguimiento del indicador ISOlucion *"Avance en la implementación de los controles de la NTC-ISO 27001:2013, en la Secretaría Distrital de Ambiente" de la vigencia 2017,* donde se implementaron 28 controles según matriz de "Priorización de los controles a implementar - sistema de gestión de la seguridad de la información SGSI anexo A de la norma ISO 27001:2013", se observa que se reportó como implementado el control A.14.2.4, se cuenta con el procedimiento gestión del cambio Código: PE03-PR04, donde se han incorporados criterios para controlar los cambios que puedan presentarse en el SGSI. Por otro lado, no han sido reportados avances sobre los demás controles de este dominio.

Recomendación:

Incluir en la matriz de priorización de controles para la implementación de la ISO 27001, la totalidad de los controles definidos para este dominio, siendo 14 controles por implementar.

1.11 Relaciones con los Proveedores (A.15)

Situación Observada: Una vez revisado el procedimiento de Gestión de Proveedores que se encuentra en elaboración, se observa que no se ha incorporado la totalidad de los criterios referentes a los controles A.15.1.2 y A.15.1.3 referente al tratamiento de la seguridad dentro los acuerdos con proveedores y a la cadena de suministro de tecnología de información y comunicación.

Recomendación:

Agilizar el diseño, implementación y aprobación del procedimiento de Gestión de Proveedores que incorpore la totalidad de requisitos de los controles del dominio, se sugiere armonizar el procedimiento con los demás subsistemas implementados en la SDA y trabajar en conjunto con los procesos gestión contractual y sistemas integrado de gestión.

1.12 Gestión de Incidentes de Seguridad de la Información (A.16)

Situación Observada: Se encuentra el plan de respuestas de incidentes de seguridad de la información con código PA03-PR14-INS3 se evidencia lo siguiente:

No cuenta con un objetivo definido, b) el documento tiene como título “instructivo plan de respuesta de incidentes de seguridad de la información” su contenido no refleja la finalidad del título establecido y c) en el numeral 2 del documento menciona un instructivo de gestión de riesgos el cual no se encuentra disponible en el aplicativo ISOlucion. No se han incorporado políticas de operación para la primera y segunda línea de defensa en

Recomendaciones:

- Revisar el documento de respuestas de incidentes de seguridad de la información con el fin de que se incluya la descripción del objetivo y que el titulo se encuentre acorde a la finalidad de este.
- Elaborar y/o cargar el documento “Instructivo de gestión de riesgos” en mención.

1.13 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio (A.17)

Situación Observada: No se evidencia avance en el diseño y planificación del plan de continuidad de los servicios tecnológicos, se observa que el proceso de Gestión tecnológica reporta como cumplimiento del control 17.1 en su indicador en el primer semestre de 2019 solo la estructuración de estudios Previos de Security Automation and Orchestration SOAR, sin reportar resultados concretos en la implementación de los controles 17.1.1, 17.1.2 y 17.1.3 referentes a la implementación y verificación.

Recomendación:

Documentar e implementar un plan de continuidad de los servicios tecnológicos y priorizar la implementación de los controles en la planeación de la próxima vigencia.

1.14 Cumplimiento (A.18)

Situación Observada: No se evidencia en los seguimientos del indicador ISOlucion *"Avance en la implementación de los controles de la NTC-ISO 27001:2013, en la Secretaría Distrital de Ambiente"* registros de avance o implementación de los (8) controles que hacen parte este dominio.

Se encuentra que no se ha realizado la revisión independiente de la seguridad de la información desde el año 2017 conforme a lo indicado el control A.18.2.1, además no se implementó la revisión del cumplimiento de las normas de seguridad en cada una de las áreas de la SDA de conformidad con el requisito control A.18.2.2.

Recomendaciones:

- Programar para el año 2020 una evaluación independiente de la seguridad de la Auditoría SGSI con el fin de dar cumplimiento al ítem 9.1 AUDITORÍAS del manual 126MSGSI y al requisito numeral 9.2 Auditoría Interna de la norma ISO 27001:2013.
- Incluir en la matriz de priorización de controles para la implementación de la ISO 27001:2013, la totalidad de los controles definidos para este dominio, siendo 8 controles por implementar.

FORTALEZAS

Excelente disponibilidad del equipo de trabajo del proceso para la atención del ejercicio de evaluación y seguimiento.

III. CONCLUSIONES:

De la verificación de los 114 controles definidos en la norma ISO 27001:2013, se observa debilidad en los registros de seguimiento (MPSI, Declaración de aplicabilidad, Indicador de gestión ISOlucion avance ISO 27001:2013", puesto que al evaluar las evidencias de su ejecución en los reportes de indicadores de las vigencias 2017, 2018 y 2019 se encontraron diferencias en el cálculo del porcentaje de avance e implementación con respecto a las actividades registradas, lo anterior por no contar con información detallada de los controles priorizados.

IV. RECOMENDACIONES GENERALES:

1. Fortalecer en las herramientas seguimiento (MPSI, Declaración de aplicabilidad, Indicador de gestión ISOlucion avance ISO 27001:2013" el detalle de los controles priorizados que le permita monitorear y evidenciar los avances e identificar las brechas para lograr su eficaz implementación.
2. Actualizar el manual 26MSGSIc conforme a las actividades y metas propuestas que realiza el proceso de Gestión Tecnológica referente a la implementación de los controles de la NTC-ISO 27001:2013.
3. Incluir en plan de trabajo las actividades parar la implementación del protocolo IPv6, dado que el término señalado por el MINTIC vence para las entidades territoriales es el 31 de diciembre de 2020.
4. Determinar y documentar por autocontrol las acciones o decisiones que se generan cuando se presenta incumplimiento o retrasos en las actividades del SGSI.
5. Considerar que las observaciones y recomendaciones que se generan por la aplicación de la Herramienta Evaluación MSPI, sean objeto de seguimiento y se incluyan acciones dentro del plan de mejoramiento del proceso.
6. Revisar los procedimientos que registran como implementados para el cumplimiento de la norma 27001:2013 en las diferentes vigencias de acuerdo con lo indicado en la guía MINTIC para la implementación del SGSI
7. Verificar periódicamente en la plataforma de Datos Abiertos Distrital que los archivos estén en los formatos correspondientes, se puedan previsualizar o descargar y se realice su actualización de acuerdo con la frecuencia establecida.
8. Definir el plan de continuidad de negocio para TI y el plan de recuperación de desastres sobre de los servicios tecnológicos que soportan los procesos de negocio.

Esta oficina estará atenta a resolver cualquier inquietud al respecto.

Atentamente,

SANDRA ESPERANZA VILLAMIL MUÑOZ
OFICINA DE CONTROL INTERNO

Anexos: N.A
c.c. Dr. Francisco Cruz Prada – Secretario Distrital de Ambiente

Revisó y aprobó:

Elaboraron: Karen Mayerly Quintero Ardila y Francisco Javier Romero Quintero Contratistas OCI
Proyectó: FRANCISCO JAVIER ROMERO QUINTERO