Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Vigencia 2020
Versión 1.0

Oficina de Tecnologías de la Información y las Comunicaciones

Secretaría Distrital de Movilidad

31 de enero de 2020

Contenido

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

1. Objetivo

Definir acciones necesarias para gestionar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, identificados en los procesos incluidos en el alcance del SGSI de la Secretaria Distrital de Movilidad.

2. Alcance

Cumplimiento al tratamiento para los riesgos de seguridad y privacidad de la información, identificados por la Secretaria Distrital de Movilidad

3. Estrategias

1. Diagnosticar estado actual en Seguridad y Privacidad de la información de la Secretaria Distrital de Movilidad.
2. Analizar de vulnerabilidades y Ethical Hacking de acuerdo a las necesidades de la entidad.
3. Analizar los riesgos encontrados.
4. Realizar el Re-test 1 de Ethical Hacking a 10 de las direcciones IP públicas y/o servicios publicados que posee la entidad expuestos en internet.
5. Elaborar análisis forense de incidentes de seguridad de la información. (Solo si es materializado)

4. Proyectos de Inversión

PROYECTÓ DE INVERSIÓN	NOMBRE DEL PROYECTO DE INVERSIÓN	CÓDIGO FUENTE FINANCIACIÓN	LÍNEA PAA	CÓDIGO RUBRO PRESUPUESTAL Y/O PROYECTO	VALOR TOTAL ESTIMADO
967	Tecnologías de información y comunicaciones para lograr una movilidad sostenible en Bogotá	118-MULTAS	SGC-112	3-3-1-15-07-44-0967-192	$ 68.400.000
			SGC-30	3-3-1-15-07-44-0967-192	$ 647.000.000

Para el desarrollo del presente plan se han contemplado los recursos necesarios en la vigencia 2020, los cuales ascienden a **SETECIENTOS QUINCE MILLONES CUATROCIENTOS MIL** ($ 715.400.000) y se encuentran en el Proyecto de

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

Inversión 967 ***"Tecnologías de información y comunicaciones para lograr una movilidad sostenible en Bogotá***"

En el contexto de la modernización tecnológica y digital del gobierno y ciudadanía digital establecida en el Plan de Desarrollo Distrital y como estrategia prioritaria en la SDM, particularmente se vienen generando estrategias e implementando acciones tendientes al logro de las metas de ciudad y del sector.

El fortalecer y modernizar el recurso tecnológico y de sistemas de información de las entidades del sector movilidad son herramientas imprescindibles para la gestión y mejoras de la movilidad en las grandes ciudades como Bogotá, integrando de forma dinámica, coordinada y sincronizada los flujos de información, flujos de documentos, flujos de materiales, vehículos, personas y flujos de recursos financieros.

Uno de los objetivos fundamentales de este proyecto de inversión es integrar y consolidar todos los componentes de TIC del sector para gestionarlos, administrarlos, utilizarlos y proyectarlos de manera unificada, transversal, interoperable y con idoneidad, entre otras. Esto traerá ventajas como optimización de recursos, economías de escala, fortalecimiento de la mayor cantidad de procesos, información a la mayor cantidad de usuarios, implementación ágil y oportuna de los componentes y robustecimiento de las competencias TIC de la SDM.

5. META 2020

Con base en las acciones a desarrollar se han definido las siguientes metas, adicionalmente, el seguimiento al cronograma propuesto se realizará por medio del Plan Operativo Anual POA con inversión y sin inversión.

Con base en las acciones a desarrollar se han definido las siguientes metas, el cual se realizará por medio del Plan Operativo Anual POA con inversión y sin inversión.

NOMBRE DEL INDICADOR	OBJETIVO	TIPO	META	FORMULA INDICADOR	FRECUENCIA DE MEDICIÓN	REGISTRO
Porcentaje de vulnerabilidades mitigadas	Verificar que las medidas implementadas para la mitigación de las vulnerabilidades es efectiva	Efectividad	Mitigar el 0 % de las vulnerabilidades detectadas	Total de vulnerabilidades mitigadas/Total de vulnerabilidades identificadas *100	Trimestral	Reportes del SOC

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

6. CRONOGRAMA

Actividad No.	Acción o Actividad	Producto	Responsable	Fecha de inicio	Fecha Fin
1	Diagnosticar estado actual en Seguridad y Privacidad de la información de la Secretaria Distrital de Movilidad.	Informe Diagnostico estado actual de la SDM.	Jefe de la Oficina de Tecnologías de la Información	15-ene-20	30-jun-20
2	Realizar test de análisis de vulnerabilidades a 75 direcciones IP y/o servicios definidos por la SDM. mediante el desarrollo del contrato 1857 de 2019 el cual tiene por objeto Realizar la gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Secretaria Distrital de Movilidad a través de un Centro de Operaciones de Seguridad (SOC).	Informe de vulnerabilidades	Jefe de la Oficina de Tecnologías de la Información	15-ene-20	30-abr-20
3	Definir los planes de mitigación de las vulnerabilidades detectadas y hacer seguimiento a estos	Informe Planes de mitigación e implementación	Jefe de la Oficina de Tecnologías de la Información	15-abr-20	30-jul-20
4	Realizar test de Ethical Hacking a 10 de las direcciones IP públicas y/o servicios publicados que posee la entidad expuestos en internet y que la entidad definirá. Mediante el desarrollo del contrato 1857 de 2019 el cual tiene por Realizar la gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Secretaria Distrital de Movilidad a través de un Centro de Operaciones de Seguridad (SOC).	Informe de vulnerabilidades	Jefe de la Oficina de Tecnologías de la Información	15-ene-20	30-abr-20

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

Actividad No.	Acción o Actividad	Producto	Responsable	Fecha de inicio	Fecha Fin
5	Realizar re-test de Ethical Hacking (plan de remediación) y apoyo a la remediación. Mediante el desarrollo del contrato 1857 de 2019 el cual tiene por objeto Realizar la gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Secretaria Distrital de Movilidad a través de un Centro de Operaciones de Seguridad (SOC). Realizar la gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Secretaria Distrital de Movilidad a través de un Centro de Operaciones de Seguridad (SOC).	Informe del Plan de Remediación	Jefe de la Oficina de Tecnologías de la Información	1-jun-20	30-sep-20
6	Realizar análisis forense digital debe ser integral y se realizará bajo un modelo metodológico reconocido internacionalmente que debe ser presentado y aprobado por la SDM. Debe tener por lo menos las siguientes fases: (solo si es materializado) A. Contexto: verificación del escenario. B. Identificación de la infraestructura. C. Recolección de evidencia. D. Análisis de la evidencia.	Informe técnico e informe gerencial	Jefe de la Oficina de Tecnologías de la Información	1-jul-20	30-dic-20
7	Prestar los servicios profesionales a la Secretaría Distrital de Movilidad para apoyar las actividades de documentación técnica y expedientes electrónicos de los conjuntos de datos y Sistemas de Información que se lideran desde la Oficina de Tecnologías de la Información y las Comunicaciones.	Documentación técnica y expedientes electrónicos de los conjuntos de datos y Sistemas de Información	Jefe de la Oficina de Tecnologías de la Información	30-abr-20	30-dic-20
8	Realizar la gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Secretaría Distrital de Movilidad a través de un centro de operaciones de seguridad (SOC).	Gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Secretaría Distrital de Movilidad	Jefe de la Oficina de Tecnologías de la Información	30-jun-20	30-dic-19

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

7. Riesgos y Controles.

Con base en el mapa de riesgos institucional se han establecido los siguientes controles a los riesgos identificados.

RIEGOS ASOCIADOS	CONTROLES EXISTENTES
1. Fallas en la infraestructura tecnológica que pueda afectar la Seguridad Digital de la Entidad.	a. Planear, registrar, evaluar, aprobar, autorizar, priorizar, ejecutar y documentar el manejo en forma controlada e integral de los cambios a la infraestructura tecnológica, comunicaciones y sistemas de información de la Secretaría Distrital de Movilidad, para preservar la disponibilidad y continuidad de los servicios soportados por las TIC, a través del cumplimiento PA04-PR04 PROCEDIMIENTO GESTIÓN DE CAMBIOS DE TIC. b. Gestionar los incidentes de Seguridad de la Información reportados conforme al procedimiento de gestión de incidentes de seguridad de la información. ~~c.~~ Herramienta Aranda, GLOBALSuite donde se documentan y se gestionan todos los incidentes de seguridad de la información, Sujeto al anexo A de la ISO/IEC 27001:2013.
2. Desconocimiento por parte de los colaboradores de la Entidad en cuanto a los principios, propósitos y aplicación de la Política de Seguridad Digital.	a. "Diseñar, desarrollar e implementar Estrategias de Sensibilización orientadas a: la transición a IPV6 y Gestión de Seguridad de la Información en la Secretaría Distrital de Movilidad" b. Realizar la capacitación y sensibilización del personal en temas de seguridad de la información c. Realizar seguimiento a la Herramienta Aranda, Herramienta GLOBALSuite, donde se documentan y se gestionan todos los incidentes de seguridad de la información, Sujeto al anexo A de la ISO/IEC 27001:2013
3. Deficiencia en la planificación de recursos y acciones y su seguimiento en cuanto a resultados esperados en Seguridad Digital de la Entidad.	a. Verificar la planificación y seguimiento de los recursos y acciones para Seguridad Digital en el Plan de Acción Institucional por parte de las dependencias responsables b. Realizar seguimiento al Plan Anual de Adquisiciones
4. Deficiencia en los mecanismos de medición de la eficacia, eficiencia y efectividad de la Política de Seguridad Digital.	a. Implementar los indicadores definidos por MinTIC para la Política de Seguridad Digital.
5. Obsolescencia tecnológica y su impacto en la Seguridad Digital.	a. Cumplir con las Políticas Específicas de la Seguridad de la Información en los numerales 5.31 y 5.32 "Política

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

RIEGOS ASOCIADOS	CONTROLES EXISTENTES
	de adquisición de hardware” y “Política de adquisición de software”.

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195