SECRETARÍA DISTRITAL DE AMBIENTE

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

Sistema de Gestión de Seguridad de la Información

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, mediante Resolución 1905 del 1 de agosto de 2019, -"Por la cual se actualizo el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018"-, artículo 4. Alineación MIG con otros modelos y sistemas de gestión. Expresa que (…) La implementación del MIG, a través de sus dimensiones y eje articulador señalados en los artículos 2 y 3 de este acto administrativo, responden a los requisitos y lineamientos normativos, a la dinámica organizacional y a mecanismos que facilitan la articulación de modelos y sistemas como lo son el MIPG, Responsabilidad social institucional, modelo de seguridad y privacidad de la información, entro otros.(…), e indica los procesos relacionados con la alineación de las políticas del MIG, indicando que (…) La política de Gobierno digital (en donde se encuentra como habilitador el Modelo de Seguridad de la Información) los Procesos (Fortalecimiento organizacional, Gestión de TI, Direccionamiento estratégico, Gestión jurídica, Comunicación estratégica, Gestión de recursos administrativos) y la política de Seguridad digital (Fortalecimiento organizacional, Gestión de TI, Direccionamiento estratégico, Gestión jurídica)(…), así mismo, en el artículo 9° por el cual se establecen las responsabilidades del Comité MIG, especialmente en los numerales 14 –"Aprobar y hacer seguimiento a la implementación de políticas de gestión y directrices en materia de Estrategia de Gobierno Digital y Seguridad de la Información en la Entidad y al Plan Estratégico de Tecnologías Información."- y 15 -"Aprobar y apoyar la implementación del plan de continuidad de la operación del Ministerio, con el fin de mitigar los riesgos asociados a una posible interrupción de la misma."-. además, el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital, de igual manera el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (…)Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.(…)

Teniendo en cuenta lo establecido en el Decreto 612 de 2018 y dando cumplimiento al mismo, se actualiza el Plan de implementación de Seguridad y Privacidad de la Información de la SDA para la vigencia 2020.

2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Desarrollar las diferentes etapas y actividades del Modelo de Seguridad y Privacidad de la Información MSPI que viene adelantando la entidad de acuerdo al ciclo PHVA (Activos de Información, gestión de riesgos, incidentes, sensibilización, requisitos legales, continuidad de negocio, acciones de mejora, articulación con MIPG y PETI, Indicadores,

Datos Personales, IPV6, aplicación de la Política Digital en su componente de seguridad todo esto alineado con la NTC/IEC ISO 27001:2013.

3. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA SDA

Consciente de las necesidades derivadas de sus actividades, la SDA implementa el Sistema de Gestión de Seguridad de la Información SGSI como una herramienta para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, administrando los riesgos, cumpliendo con la legislación vigente, y generando una cultura de seguridad de la información en las partes interesadas.

4. OBJETIVOS DE LAS POLITICAS DE SEGURIDAD Y PRIVACIDAD

OBJETIVO GENERAL

Mantener la confidencialidad, integridad, disponibilidad de los activos de información, y la protección de datos personales**,** mediante la gestión los riesgos, que permita establecer un marco de confianza a las partes interesadas en concordancia con la misión y visión de la entidad.

OBJETIVOS ESPECÍFICOS:

1. Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad, mediante la implementación de controles en los procesos de la entidad de manera coordinada con las partes interesadas.
2. Gestionar los riesgos asociados con la perdida de confidencialidad, integridad, disponibilidad y privacidad de la información dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI).
3. Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de sus derechos.
4. Sensibilizar y entrenar al personal de la entidad en el Sistema de Gestión de Seguridad de la Información (SGSI).

5. ALCANCE DEL SGSI DE LA SDA

El sistema de Gestión de la Seguridad de la Información (SGSI) de la Secretaría Distrital de Ambiente, cubre todos los procesos y procedimientos asociados al Sistema Integrado de Gestión, siguiendo el estándar de la norma NTC-ISO-IEC 27001:2013 y los elementos complementarios del Modelo de Seguridad y Privacidad de la Información MSPI orientados por MINTIC, la política Digital y la guía de Riesgos dado por el DAFP

6. PLANFICACION, CONTROL OPERACIONAL Y ARTICULACIÓN DEL MSPI

Las etapas definidas para el desarrollo y la implementación del Subsistema de Gestión de Seguridad de la Información son:

1. Planear y documentar el sistema
2. Implementar el sistema
3. Evaluar el sistema a través de auditorías internas y externas
4. Mejorar continuamente la eficacia del sistema a través de del análisis de datos

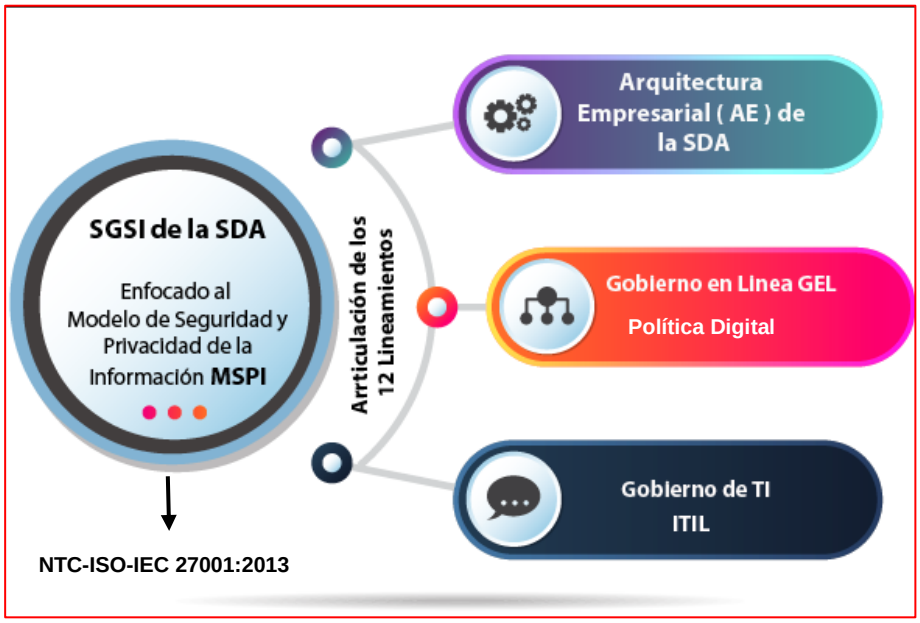

FIGURA 1: Secretaria Distrital de Ambiente SDA 2019

7. PLAN DE IMPLEMENTACIÓN DEL MSPI

El Plan de implementación para el cumplimiento, seguimiento y control de Seguridad y Privacidad de la Información se disgrega en el siguiente cronograma y se le hace seguimiento mes a mes. Se tienen las recomendaciones dadas por la oficina de control interno luego de la revisión del SGSI durante el 2019 y se alinea a lo descrito en el PETI y el PAA

PLAN DE IMPLEMENTACIÓN DEL MSPI(SGSI) DE LA SDA PARA LA VIGENCIA 2020							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
Activos de Información 2020	Aceptación de Activos de Información	Revisión con todos los responsables de la aceptación de la matriz de activos Aprobación final de todas las matrices y consolidación para posterior publicación	Matriz Final de Activos de Información	Líder de Gestión Documental, Líder de Transparencia, Líder de Seguridad de la Información, Líder Datos Abiertos, Líder SIG para Seguridad	X		
	Publicación de Activos de Información	Publicación de la matriz de Activos	Matriz de Activos en el portal de la entidad	Líder Seguridad de la Información, Líder de Gestión Documental Líder de Transparencia Dependencia de comunicaciones y Web Master	X		
	Levantamiento de Activos de Información en el Módulo de Isolucion.	Los enlaces SIG de la entidad ingresen la información al módulo de seguridad de la información en isolucion	Módulo de Seguridad de isolucion con la información de las matrices.	Líderes SIG de cada Área de la entidad	X		
	Revisión y aceptación de los activos de información subidos a la plataforma isolución por parte de seguridad de la información	Revisión y aceptación de los activos	Revisión y aceptación de los activos subidos por parte de los líderes SIG al módulo de seguridad de la información	Líder de Seguridad de la Información	X		
Gestión de Riesgos 2020	Actualización de lineamientos de riesgos 2020	Actualización de la metodología de riesgos asociado a seguridad de la información	Documento de riesgos actualizado	Líder SIG de seguridad de la información, Líder Seguridad de la Información. Líder Riesgo de la SDA	X		
	Actualización e Identificación de Riesgos de Seguridad y Privacidad de la Información, y Seguridad Digital a 2020	Documento con la Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital a 2020	Documento con la identificación, Análisis y Evaluación de Riesgos	Enlace SIG de los procesos Líder Seguridad de la Información. Administrador del riesgo de la SDA		X	
	Aceptación de Riesgos Identificados 2020	Documento con la realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Documento Final	Enlace SIG de los procesos Líder Seguridad de la Información. Administrador del riesgo de la SDA		X	

PLAN DE IMPLEMENTACIÓN DEL MSPI(SGSI) DE LA SDA PARA LA VIGENCIA 2020							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
		Aceptación, aprobación Riesgos identificados y planes de tratamiento	Documento oficial de aprobación			X	
	Publicación de Matriz de Riesgos 2020	Publicación Matriz de riesgos	Matriz de riesgos publicada	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de comunicaciones y Web Master		X	
	Seguimiento Fase de Tratamiento 2020	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Documento con el seguimiento	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de comunicaciones y Web Master		X	
	Evaluación de riesgos residuales 2020	Evaluación de riesgos residuales	Documento con la evaluación de los riesgos residuales	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de comunicaciones y Web Master		X	
	Mejoramiento de estado de riesgos de acuerdo con el PHVA	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Documento Final	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de comunicaciones y Web Master		X	
	Actualizar el procedimiento de incidentes de seguridad de la información de la SDA de acuerdo a las últimas recomendaciones dadas en ciberseguridad 2020	Desarrollar las actualizaciones a que sean pertinentes	Documento Final de Incidentes con las actualizaciones pertinentes	Líder Seguridad informática Líder de Seguridad de la Información		X	
	Gestionar los incidentes de Seguridad de la Información identificados		Continuar con la gestión de incidentes	Líder Seguridad informática	X	X	X

PLAN DE IMPLEMENTACIÓN DEL MSPI(SGSI) DE LA SDA PARA LA VIGENCIA 2020							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
Gestión de Incidentes de Seguridad de la Información 2020	Contacto con CSIRT, COLCERT y demás grupos de interés	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno, seguir en contacto con los grupos de interés en ciberseguridad 2020	Boletenis socializados	Líder Seguridad informática	X	X	X
	Eventos/vulnerabilidades 2020	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados al SGSI	Gestión de Monitoreo y reporte	Líder Seguridad informática	X	X	X
Plan de Sensibilización de Seguridad y Privacidad de la Información	Actualizar Plan de Sensibilización de Seguridad y Privacidad de la Información 2020	Elaborar el documento del Plan	documento Final con el Plan de sensibilización 2020	Líder Seguridad de la Información	X		
	Aplicar el Plan de Sensibilización de Seguridad y Privacidad de la Información 2020	Aplicar el Plan	Evidencias del Plan aplicado	Líder Seguridad de la Información		X	X
	Analizar el Plan de Sensibilización de Seguridad y Privacidad de la Información 2020 que fue aplicado	Analizar los resultados del Plan	Informe con el Análisis de los resultados del Plan	Líder Seguridad de la Información			X
Requisitos Legales de Seguridad de la Información	Cláusulas de verificación de Requisitos Legales de Seguridad de la Información	Coordinar con el líder SIG de seguridad la revisión y envío de las cláusulas a contractual	Clausulas en contractual	Líder SIG seguridad de la información. Líder de seguridad de la información Abogados Contractual		X	
Plan de Continuidad del Negocio	Aportar los componentes de seguridad de la información a documento de del Análisis de Impacto de Negocio	Análisis de Impacto de la Operación por una posible interrupción de los servicios de seguridad	Documento con el análisis de impacto	Líder de seguridad de la información Líder de Continuidad de Negocio de la SDA Líder de infraestructura de la SDA		X	
Acciones correctivas y	Revisión de las observaciones dadas por	Revisar los documentos enviados por OCI y Aplicar de acuerdo lo	Plan de trabajo o de mejora en SGSI	Líder de seguridad de la información		X	

PLAN DE IMPLEMENTACIÓN DEL MSPI(SGSI) DE LA SDA PARA LA VIGENCIA 2020							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
Notas de mejoras SGSI	Oficina de Control Interno I sobre el SGSI y su aplicación	establecido por MINTIC, ISO 27001 y Política Digital		Equipo			
Planeación MSPI Gobierno Digital 2020	**Gobierno Digital-** **Política Digital 2020**	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información 2020	Autodiagnóstico de la política de Seguridad y Privacidad de la Información	Líder de seguridad de la información	X		
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo el resultado del instrumento de MINTIC para la vigencia 2020.	Manual del SGSI Documento de planeación herramienta WBS	Líder de seguridad de la información		X	
Controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013	Desarrollo, implementación y actualización de los controles faltantes y existentes referenciados en el anexo A de la ISO 27001.2013	Implementación de los controles ISO 27001	Líder de seguridad de la información Equipo SIG	X	X	X
Indicadores SGSI 2020	Provisión de información a los indicadores de medición del SGSI	Reportar indicadores en las vigencias trimestrales y semestrales solicitadas 2020	indicadores del SGSI 2020	Líder de seguridad de la información Enlace SIG Administración de indicadores del la SDA	X	X	X
Vulnerabilidades	Ejecutar y analizar las pruebas de vulnerabilidades con la herramienta TENABLE	Ejecutar las pruebas de vulnerabilidades de la entidad y analiza sus resultados	Pruebas y reportes de Tenable	Líder de seguridad Informática	X	X	X
	Enviar el plan de remediación de vulnerabilidades a el Administrador de la	Enviar documento de remediación y hacer seguimiento y verificación	plan de remediación de vulnerabilidades	Líder de seguridad Informática	X	X	X

PLAN DE IMPLEMENTACIÓN DEL MSPI(SGSI) DE LA SDA PARA LA VIGENCIA 2020							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
	solución de software y verificar que se realizó adecuadamente la remediación.						
Protección de datos personales	Revisión de bases de datos	Revisión de matriz de acuerdo a la 1581 y demás normatividad	matriz de activos de información en su componente de privacidad	Líder de seguridad de la información		X	
Estrategias De Innovación En Ciberseguridad	Nuevas estrategias de innovación sobre ciberseguridad para la SDA	Continuar estudiando, probando, testeando, y aplicando nuevas herramientas de seguridad asociadas a seguridad de la información	informaciones asociadas a inteligencia artificial y Machine learning	Líder de seguridad de la información	X	X	X
implementación del estándar IPV6	Continuar con la implementación del estándar IPV6 para la SDA	Desarrollar reunión para revisar el estado actual de implementación de IPV6 a 2020 y cronograma de implementación 2020 de IPV6	Documento de estado actual y cronograma de implementación	Líder de seguridad de la información Administradores de infraestructura de TI Webmaster	X	X	
Seguridad en la Nube y Estructuración	Seguridad en nube de las aplicaciones de la entidad que están en Complete Cloud o Hybrid Cloud	Desarrollar estrategia para proteger las aplicaciones en Cloud	Aplicaciones en Cloud	Líder de seguridad de la información	X	X	X
Pruebas de Efectividad del MSPI 2020	Realizar las pruebas de efectividad del MSPI sobre finales del 2020	Desarrollar y aplicar las pruebas de efectividad del MSPI 2020	pruebas de efectividad 2020	Líder de seguridad de la información Administradores de infraestructura de TI	X	X	X

8. RECOMENDACIONES

Es importante que se cuente con un equipo de recurso humano adecuado capaz y suficiente en seguridad de la información y seguridad informática para llevar a buen término el cronograma propuesto para 2020

Se debería separar en roles distintos la Seguridad Informática de la SDA y la Seguridad de la Información las cuales son completamente distintas.

Debe existir mayor integración entre los oficiales de Seguridad de la Información, Oficial de Cumplimiento (Trasparencia) y Oficial de Datos Personales (Privacidad)

La integración de seguridad de la seguridad de la información debe ser multidisciplinar y recaer en todos los funcionarios y contratistas de la SDA.

Luego de subsanar las observaciones pertinentes de la OCI se debe programar la primera auditoria NTC- ISO 27001:2013 para la vigencia 2020