PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SCRD – VIGENCIA 2021

1. OBJETIVO

Definir la planificación de las actividades orientadas a gestionar y fortalecer el tratamiento de los riesgos asociados a la seguridad y privacidad de la información, que es generada, tratada y custodiada por la Secretaria de Cultura Recreación y Deportes de ahora en adelante denominada SCRD en el presente documento; con el fin preservar la confidencialidad, integridad y disponibilidad, de la información en la entidad.

1.1 OBJETIVOS ESPECÍFICOS

- Fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información de la SCRD, mediante la implementación y mejora de los controles de seguridad alineados con el Modelo de seguridad y privacidad de la información y la ISO 27001:2013.
- Definir y divulgar las políticas, lineamientos, procedimientos y buenas prácticas recomendaciones para establecer una cultura organizacional de Seguridad y Privacidad de la Información en la SCRD.
- Realizar el seguimiento a las acciones pertinentes a reducir las brechas de cumplimiento de acuerdo al autodiagnóstico del MIPG relacionado al habilitador transversal de seguridad y privacidad de información.
- Definir y gestionar y monitorear los riesgos de Seguridad y Privacidad de la Información en la SCRD.
- Apoyar la evaluación y documentación de la efectividad de los controles de Seguridad y privacidad de la Información identificados en la Declaración de Aplicabilidad que soportan el modelo de Seguridad de la Información establecido en la Secretaría Distrital de Cultura, Recreación y Deporte

2. DEFINICIONES

- **Activo de información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma, el cual tiene valor para la SCRD por lo tanto para ello se tienen contemplados los siguientes activos de información: personas, información/dato, hardware, software, redes, infraestructura y servicios.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Seguridad de la información**: Conjunto de medidas que toman las personas y las organizaciones, que les permiten resguardar y proteger los activos de información, preservando su Confidencialidad, Integridad y Disponibilidad.
- **Confidencialidad:** Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
- **Disponibilidad:** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Integridad:** Garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- **Sistema de Gestión de Seguridad y privacidad de la información**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

3. MARCO LEGAL

Dentro del marco legal más relevante para justificar el presente plan de seguridad y privacidad de la información se encuentran las siguientes normas:

- **Ley 1437 de 2011, Capítulo IV**, "utilización de medios electrónicos en el procedimiento administrativo". "Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."
- **Ley 1581 de 2012**, g) Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento". Artículo 17, ítem d: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".
- **Ley 1712 de 2014**, "principio de transparencia": "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley".

  Artículo 7: "Disponibilidad de la información" "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

Título III “Excepciones acceso a la información” “Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.”

- **Conpes 3854 de 2016**, objetivo general “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.
- **Decreto 1008 de 2018** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". **ARTÍCULO 2.2.9.1.1.3.** Principios. “Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano”.
- **Decreto 612 de 2018**, artículo 1. “Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web.”

4. GENERALIDADES

El presente plan está orientado a mejorar por medio de la implementación acciones concretas al Sistema de Gestión de Seguridad y Privacidad de la Información de la SCRD; para tal fin es necesario mencionar que estas acciones están enmarcadas intervenir los 3 componentes del modelo (Personas, Procesos y Tecnología).

- **Compromiso:** Para la ejecución del plan es necesaria la participación de los diferentes niveles de decisión de la SCRD (estratégico, táctico y operativo), especialmente para la valoración de procesos frente a las normas ISO 27001/2:2013, así como también se asume el compromiso y el involucramiento de todos los colaboradores de la SCRD.
- **Población Objetivo:** Para asegurar el éxito en la ejecución del plan es prioritario involucrar a las personas que ejercen responsabilidades de seguridad de la información en la SCRD las cuales están identificadas en la matriz de roles y responsabilidades del Sistema de Gestión de Seguridad y Privacidad de la Información; así como también todos aquellos colaboradores que deben apoyar y/o asistir a las reuniones y entrevistas que se llevaran a cabo para el levantamiento de la información requerida y que por su actuar están directa o indirectamente relacionados con los procesos y procedimientos establecidos de Seguridad de la Información.
- **Duración:** El tiempo estimado para la ejecución del plan es de 11 meses contados a partir de la aprobación del presente plan de trabajo.
- **Seguimiento:** Se establece un seguimiento trimestral a la ejecución de las actividades propuestas en el plan.

5. PLANIFICACIÓN DE ACTIVIDADES

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la SCRD 2021			Seguimiento del Plan	
Categoría MIPG	**Actividad**	**Resultados Esperados**	**F Inicial**	**F Final**
Implementación MIPG 2021	Definición y seguimiento del plan de seguridad y privacidad de la información y tratamiento de riesgos 2021	Definición del Plan de tratamiento de Riesgos de seguridad, privacidad de la información	1/12/2020	30/01/2021
Definición del marco de seguridad y privacidad de la información y de los sistemas de información	Actualización del perfil de riesgos de Seguridad digital y protección de datos personales	Actualización del perfil de riesgos de seguridad y privacidad de la información	30/07/2021	30/09/2021
		Definición de riesgos de protección de datos personales	1/05/2021	30/07/2021
		Definición del plan de tratamiento de riesgos de seguridad, privacidad de la información y protección de datos personales en la entidad	30/07/2021	15/08/2021
Plan de seguridad y privacidad de la información y de los sistemas de información	Implementación del plan de tratamiento de riesgos de seguridad digital de la SCRD	Apoyar la gestión de solicitud de contratación de mantenimiento de equipos UPS y ejecución del mismo	3/02/2021	15/03/2021
		Realizar seguimiento al plan de mantenimiento de infraestructura TIC y equipos de cómputo para la vigencia 2021 I semestre	1/01/2021	30/06/2021
		Realizar seguimiento al plan de mantenimiento de infraestructura TIC y equipos de cómputo para la vigencia 2021 II semestre	30/06/2021	30/12/2021
		Diagnóstico del cumplimiento del dominio **A11 SEGURIDAD FÍSICA Y DEL ENTORNO** de la ISO 27001:2013	3/02/2021	15/06/2021
		Planeación e Implementación de los controles de seguridad físicos del data center principal y centro de cableado	16/06/2021	30/12/2021
		Definición de ANS (Acuerdo de Nivel de Servicio) de disponibilidad del servicio con el proveedor de internet	3/02/2021	15/03/2021
		Revisión y actualización procedimiento de Gestión de sistemas de información	3/02/2021	15/06/2021
		Actualización e implementación del programa de Cultura de seguridad y privacidad de la información	3/02/2021	1/03/2021
		Revisar y actualizar la política de buen uso de los activos de información	3/02/2021	30/06/2021
		Revisión cumplimiento del MSPI (Modelo de Seguridad y privacidad de la Información).	3/02/2021	30/12/2021
		Depuración de usuarios en las bases de datos gestionadas por GIS	3/02/2021	30/12/2021
		Realización, verificación y restauración de las Copias de Seguridad de los servidores TIC (Aplicaciones, Almacenamiento) de	3/02/2021	30/12/2021

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la SCRD 2021			Seguimiento del Plan	
Categoría MIPG	**Actividad**	**Resultados Esperados**	**F Inicial**	**F Final**
		acuerdo con lo establecido en el Instructivo de copias de seguridad.		
		Seguimiento con la atención y solución de tickets registrados en la mesa de servicios de acuerdo a lo establecido el el procedimiento de Soporte Técnico, relacionados con seguridad y privacidad de la información	3/02/2021	30/12/2021