PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2023

Secretaría Distrital de Desarrollo Económico
Bogotá, Diciembre de 2022

TABLA DE CONTENIDO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Objetivo general

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Secretaría Distrital de Desarrollo Económico para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en el presente plan para la vigencia 2023.

2. Objetivos específicos

- Definir las actividades a realizar en el año 2023 para realizar el cierre de brecha establecido en el autodiagnóstico del MSPI para el año 2022.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Seguridad de la Información.
- Priorizar los proyectos a desarrollar para la correcta implementación del Sistema de Seguridad de la Información.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

3. Alcance

El Plan de Seguridad de la Información comparte el alcance definido dentro de la Política de Seguridad de la Información, donde se indica que es transversal a todos los procesos y procedimientos institucionales de la Secretaría Distrital de Desarrollo Económico (en adelante SDDE).

Aplica a todos los usuarios internos y externos de la Secretaría de Desarrollo Económico (servidores públicos, funcionarios vinculados a la planta permanente y provisional, contratistas, consultores, pasantes, proveedores de bienes, entidades del Estado, entes

de control) y otros terceros que desempeñen alguna actividad en las instalaciones de la Secretaría Distrital de Desarrollo Económico o a nombre de esta.

4. Glosario

- Activo de información: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2018]
- Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Contratista: Persona natural o jurídica contratada por la SDDE para la adquisición de una obra, bien o servicio, no perteneciente al régimen laboral.
- Control: comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- Copias de Seguridad: Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla y disponerla en caso de que ocurra un fallo que afecte a esta
- Dato personal: hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Información: Es un activo de valor que hace parte de la SDDE, por la cual asume funciones como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato corporativo (tecnológico, administrativo, financiero, contable, entre otros), propio

o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado.

- Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.
- Modelo Integrado de Planeación y Gestión- MIPG: el Sistema de Gestión que deben aplicar las entidades públicas de la Rama ejecutiva, el cual integra y articula los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad con el Sistema de Control Interno.
- Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- Política de Seguridad de la Información: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene el conjunto de lineamientos y procedimientos que deben ser implementados para gestionar la seguridad de la información.
- Seguridad informática: conjunto de medidas técnicas que son implementadas para asegurar los recursos e información contenida en los componentes tecnológicos institucionales.
- Seguridad de la información: conjunto de medidas que buscan la protección de la información física, electrónica, digital del acceso, uso, divulgación o destrucción no autorizada.
- Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

5. Marco Normativo

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Decreto 454 del 21 de marzo de 2020. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la política de gestión de la información estadística a las políticas de gestión y desempeño institucional.
- Directiva Presidencia 03 de 15 de marzo de 2021: Lineamientos para el Uso de Servicios
- en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.
- Decreto 767 de 2022 “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"'
- Ley 1712 del 06 de marzo de 2014, “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Ley 1915 del 12 de julio de 2018, “Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”.
- Decreto 1074 del 26 de mayo de 2015. “Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo”. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1083 del 26 de mayo de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, (“11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital)
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano.

- Decreto 612 de 4 de abril de 2018. “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.”
- Decreto 1008 del 14 de junio 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. “
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP
- Resolución 004 del 28 de Noviembre de 2017 "Por la cual se modifica la Resolución 305 de 2008 de la Comisión Distrital de Sistemas"
- CONPES 3995 del 1 de julio de 2020. Política Nacional de Confianza y Seguridad Digital.
- Resolución 1519 de 2020: “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
- Ley 1273 del 05 de enero de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado: de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
- Ley Estatutaria 1581 del 17 octubre de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”
- NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

6. Estado actual de la entidad respecto al sistema de gestión de seguridad de la información

La Secretaría Distrital de Desarrollo Económico a través de la Subdirección de Informática y Sistemas viene realizando un ejercicio de fortalecimiento a las necesidades propias de la estrategia de Gobierno Digital orientada en la Nació por el MinTIC y en el distrito por la Alta Consejería de TICs.

Dentro de este ejercicio se está trabajando en la actualización de los diagnósticos frente a sus diferentes componentes y en la ejecución del ejercicio de planeación de los instrumentos respectivos y específicamente para este caso la estrategia de seguridad digital de la entidad.

Instrumento MSPI

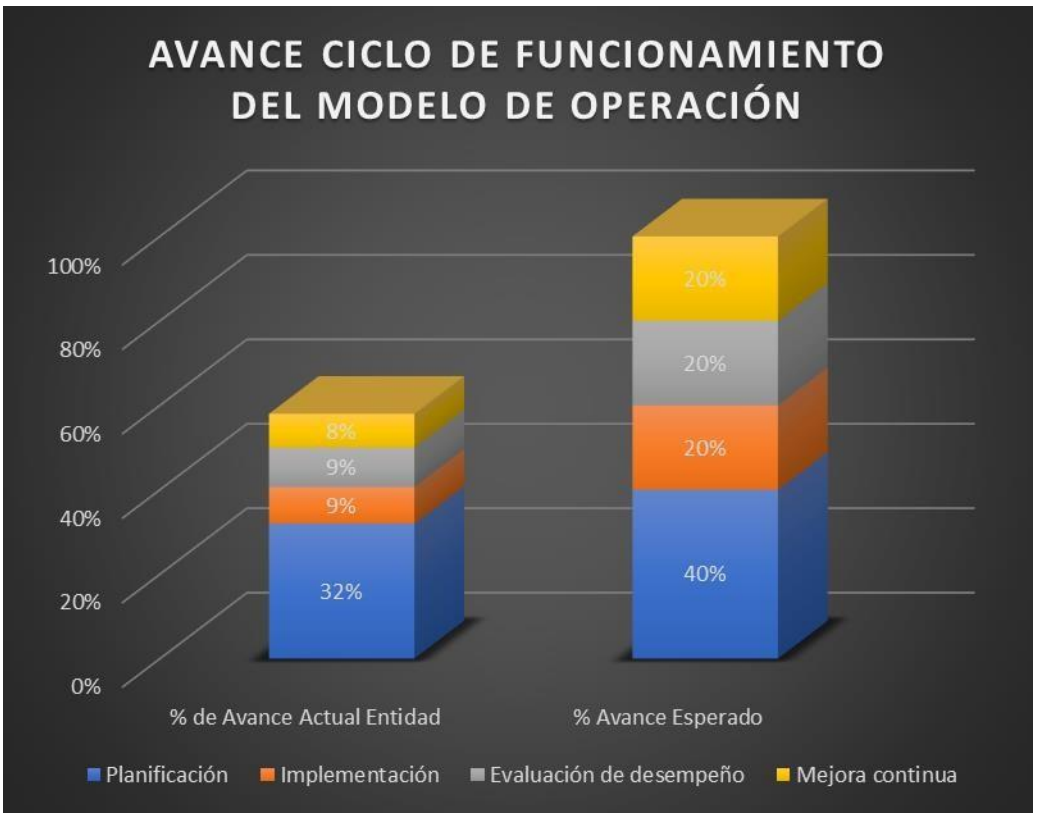
En el diagnóstico respectivo se adelantó la actualización del instrumento de autodiagnóstico del MSPI con los siguientes resultados:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	43	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	76	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	60	100	EFECTIVO
A.9	CONTROL DE ACCESO	39	100	REPETIBLE
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	79	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	57	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	69	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	27	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	EFECTIVO
A.18	CUMPLIMIENTO	50	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**53**	**100**	EFECTIVO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	32%	40%
	Implementación	9%	20%
	Evaluación de desempeño	9%	20%
	Mejora continua	8%	20%
TOTAL		58%	100%



Instrumento FURAG

De igual forma se tuvo en cuenta la medición FURAG adelantada para el año 2021 en donde se detectaron brechas importantes en la actualización y formalización de documentos que son parte de la estructura de planeación de la estrategia de Seguridad de Información de la entidad y por lo tanto en su ejecución y seguimiento.

Revisando específicamente la información concerniente a las responsabilidades directas o indirectas de los procesos de la Subdirección de Informática y Sistemas de la SDDE se encontró que a pesar de que el índice de desempeño para la entidad fue del 86.6 sobre 100, en aspectos específicos de gobierno digital y seguridad de la información estos resultados fueron menores:

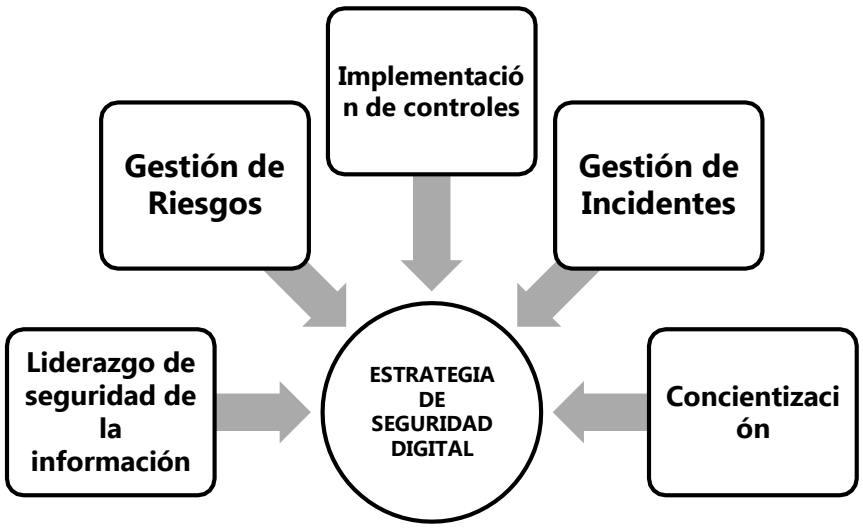
- I21GOBIERNO DIGITAL **Fortalecimiento de la Seguridad y Privacidad de la Información 62.4 sobre 100.**
- I82 GOBIERNO DIGITAL Procesos seguros y eficientes 67.8 sobre 100.
- I83 GOBIERNO DIGITAL Toma de decisiones basadas en datos 70.5 sobre 100.
- I84 GOBIERNO DIGITAL Impulso en el desarrollo de territorios y ciudades inteligentes 42.2 sobre 100.
- I85 GOBIERNO DIGITAL Uso y apropiación de los Servicios Ciudadanos Digitales 65.0 sobre 100.
-

Teniendo en cuenta estos resultados se puede evidenciar que se debe trabajar en la generación de actividades que permitan realizar el cierre de estas brechas para que la gestión de tecnología de la entidad se realice de manera eficiente, segura y controlada.

7. Estrategia de seguridad digital de la SDDE

La Secretaría Distrital de Desarrollo Económico establece una estrategia de seguridad digital en la que se integran desde la Política de Seguridad y Confidencialidad de la Información, los procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes establecido.

Por lo anterior, La Secretaría Distrital de Desarrollo Económico define la estrategia general de seguridad digital con base en las siguientes estrategias específicas:



7.1. Estrategias específicas de seguridad digital de la SDDE

A continuación, se describe el objetivo de cada una de las estrategias específicas que hacen parte de la estrategia general de seguridad digital de la SDDE de acuerdo con lo recomendado por MinTIC:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la SDDE.

7.2. Cronograma de actividades

Con base en la priorización adelantada, la cual corresponde al cierre de la brecha presentada en el autodiagnóstico del MSPI y FURAG, se presenta a continuación el plan de trabajo para el año 2023:

item	ACTIVIDAD A REALIZAR	RECOMENDACIÓN	FECHA	RESPONSABLE
1	**Actualización de la política y aprobación por parte del comité de gestión de la entidad**	Realizar la actualización y formalización de la política de seguridad de la información.	Diciembre 2022	Funcionarios de planta y contratistas con esta obligación
2	**Elaboración, aprobación e implementación plan operacional de seguridad y privacidad de la información**	Elaborar el plan operacional de seguridad y privacidad de la información de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.	Enero 2023	Funcionarios de planta y contratistas con esta obligación
3	**Actualización del manual de seguridad de la información con los dominios estipulados por la Política de seguridad de la información de la entidad**	Implementar procedimiento de etiquetado de la información e incluirlo en el manual de seguridad de la información Incluir procedimiento de control de cambios en el manual de seguridad de la información Incluir procedimiento para proveedores y seguimiento al cumplimiento en el manual seguridad de la información Incluir política control de acceso con este componente en el manual de seguridad de la información Incluir la política de propiedad intelectual en el manual de seguridad de la información Incluir la política de controles criptográficos en el manual de seguridad de la información Incluir procedimiento de borrado en el manual de seguridad de la información Documentar política de escritorio limpio en el manual de seguridad de la información Incluir política de respaldo de información en el manual de seguridad de la información Incluir procedimiento de gestión de incidentes en manual de seguridad de la información Incluir en el manual de seguridad de la información que documente los controles de transferencia de la información Incluir procedimiento criptografía de las comunicaciones en manual de seguridad de la información Crear procedimiento para autorización de cambios en registros y manejo de logs dentro del manual de seguridad Incluir procedimiento de actualización de software en el manual de seguridad de la información	Enero 2023	Funcionarios de planta y contratistas con esta obligación
4	**Inclusión de socialización de seguridad de la información en el plan de comunicaciones de la SIS para el año 2023**	Comunicar permanentemente sobre los lineamientos de seguridad de la información tanto a funcionarios como contratistas de la entidad	Enero 2023	Funcionarios de planta y contratistas con esta obligación
5	**Articulación de un plan de capacitación con Alta Consejería de Tics, Mintic, y otros, sobre seguridad digital**	Fortalecer las capacidades en seguridad digital de la entidad estableciendo convenios o acuerdos con otras entidades en temas relacionados con la defensa y seguridad digital.	Febrero 2023	Funcionarios de planta y contratistas con esta obligación
6	**Implementación y socialización de un canal de reporte anónimo sobre incidentes o amenazas de seguridad de la información**	Implementar canales confidenciales de comunicación para presentar información sobre amenazas sobre la seguridad de la información de la entidad	Febrero 2023	Funcionarios de planta y contratistas con esta obligación
7	**Inclusión de normas sobre seguridad de la información en un normograma corporativo**	Elaborar un compendio de las normas que aplican al proceso de TIC de la entidad e incluirlo en el normograma de la entidad	Febrero 2023	Funcionarios de planta y contratistas con esta obligación
8	**Definición de indicadores para el sistema de seguridad y privacidad de la información de la entidad**	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.	Marzo 2023	Funcionarios de planta y contratistas con esta obligación
9	**Apoyo en la elaboración y actualización de un procedimiento de gestión y tratamiento de datos personales**	Realizar la elaboración y/o actualización de la política de gestión y tratamiento de datos personales en la plataforma tecnológica de la entidad.	Marzo 2023	Funcionarios de planta y contratistas con esta obligación

item	ACTIVIDAD A REALIZAR	RECOMENDACIÓN	FECHA	RESPONSABLE
10	**Inclusión de lineamientos para el aseguramiento de la información en la estrategia de continuidad de negocio de la entidad**	Incluir lineamientos de seguridad y privacidad de la información en la estrategia de continuidad de negocio de la entidad.	Abril 2023	Funcionarios de planta y contratistas con esta obligación
11	**Diseño de un manual de adquisición, desarrollo y mantenimiento de sistemas de información seguros**	Documentar la seguridad de servicios de las aplicaciones en redes públicas Documentar el procedimiento de protección de transacciones Creación de lineamiento de desarrollo seguro Creacipón de un procedimiento para el control de cambios en sistemas Revisión técnica de las aplicaciones después de cambios en la plataforma de operación Principios de construcción de sistemas seguros Implementar lineamientos de seguridad de datos de prueba	Mayo 2023	Funcionarios de planta y contratistas con esta obligación
12	**Gestión de riesgos y adopción de la guía para la identificación de infraestructura crítica cibernética**	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética. Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.	Mayo 2023	Funcionarios de planta y contratistas con esta obligación
13	**Implementación de la guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en entidades públicas.**	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en entidades públicas.	Junio 2023	Funcionarios de planta y contratistas con esta obligación
14	**Participación en las mesas de construcción y sensibilización del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.**	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en las mesas de construcción y sensibilización del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.	Junio 2023	Funcionarios de planta y contratistas con esta obligación
15	**Diseño y ejecución de ejercicios de simulación de incidentes de seguridad - hacking etico y demás.**	Efectuar evaluaciones de vulnerabilidades informáticas. Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad.	Agosto 2023	Contratistas a cargo
16	**Participación en el diseño e implementación de un plan sectorial de protección de la infraestructura crítica cibernética**	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.	Octubre 2023	Funcionarios de planta y contratistas con esta obligación
17	**Realización periódica de ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos**	Realizar periódicamente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos.	Octubre 2023	Funcionarios de planta y contratistas con esta obligación
18	**Actualización Autodiagnostico MSPI**	Realizar un diagnóstico de seguridad y privacidad de la información para la vigencia, mediante la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).	Noviembre 2023	Contratista a cargo y Funcionarios de Planta
19	**Gestión de riesgos de seguridad de la información**	Identificar los riesgos de seguridad y privacidad de la información de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, valorarlos y actualizarlos mediante un proceso de mejora continua. Establecer controles para evitar la materialización de riesgos de seguridad y privacidad de la información. Identificar factores sociales que pueden afectar negativamente el cumplimiento de los objetivos institucionales. Desde el sistema de control interno efectuar su verificación. Identificar factores tecnológicos que pueden afectar negativamente el cumplimiento de los objetivos institucionales. Desde el sistema de control interno efectuar su verificación. Hacer seguimiento a los riesgos de seguridad de la información	Noviembre 2023 Junio - noviembre 2023	Funcionarios de planta y contratistas con esta obligación
20	**Implementación de ejercicios de seguimiento de brechas de seguridad de la información**	Realizar informes periódicos con el seguimiento a las brechas de seguridad detectadas por la entidad de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información	Junio - noviembre 2023	Funcionarios de planta y contratistas con esta obligación

8. Responsables

Los responsables de la implementación del siguiente plan se establecen junto con sus roles en la Política de Seguridad y Privacidad de la Información de la SDDE. A continuación, se describen:

8.1. Alta dirección

Asignar y aprobar los recursos humanos y económicos para la implementación de la Política de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información.

8.2. Comité Institucional de gestión y desempeño

Es la instancia encargada de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con el Modelo Integrado de Planeación y Gestión MIPG y el Modelo de Seguridad de Seguridad y Privacidad de la Información.

8.3. Subdirección de Informática y Sistemas

La Subdirección de Informática y Sistemas es responsable de administrar y controlar el acceso a los recursos de la plataforma tecnológica en la SDDE de acuerdo con la descripción del cargo. Sus responsabilidades frente al SGSI son:

- Monitorear a través de las herramientas tecnológicas de la Entidad el comportamiento del uso del servicio de Internet.
- Verificar qué usuarios y/o contratistas tienen acceso remoto a los recursos de la Entidad.
- Asegurar el correcto funcionamiento y la disponibilidad que la Entidad requiere del servicio de Internet, sobre el cual se deben aplicar los controles que se definan.
- Generar informes del uso del servicio, como medida preventiva de seguridad que permita tomar decisiones y realizar ajustes de configuración.

- Gestionar los accesos a los servicios o sistemas de información que dependan de la SDDE, y solicitar aquellos que deban ser tramitados ante externos, de acuerdo con lo indicado por los responsables o dueños de los sistemas de información.
- Implementar y gestionar los controles de seguridad sobre los activos de información de la entidad
- Coordinar las acciones junto con el Oficial de seguridad o quien haga sus veces, para garantizar la seguridad y privacidad de los activos de información de la entidad.

8.4. Directores, Subdirectores y Jefes de Dependencia

Asegurar que todos los procedimientos de seguridad de la información se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información.

8.5. Líder de procesos y su información

Los responsables de la Información en la Entidad deben valorar su información, reconocer los riesgos a que se expone y cuidar de que se provean los mecanismos necesarios para mitigar los riesgos a niveles aceptables. Frente a las responsabilidades de seguridad de la información, están:

- Identificar los activos, riesgos y controles para el manejo de la información.
- Sugerir posibles ajustes para la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Apoyar al Equipo de Seguridad de la Información en la identificación de los requerimientos de Seguridad de la Información.
- Participar en las Auditorías del Sistema de Gestión de Seguridad de la información.
- Solicitar los accesos a los sistemas de información sobre los cuales sean responsables de acuerdo con los lineamientos definidos por la Subdirección de Informática y Sistemas.
- Informar de manera oportuna a la Subdirección de Informática y Sistemas cuando el funcionario ha dejado de pertenecer a la Entidad, inicie su periodo

de vacaciones o licencia, o cuando algún usuario tenga novedades en sus roles o funciones, para revocar o modificar las credenciales asignadas para las aplicaciones y servicios a los cuales tiene acceso.

8.6. Oficial de seguridad de la Información.

El Oficial de Seguridad de la Información de la Entidad es responsable de las siguientes actividades:

- Estructurar, orientar, liderar la implementación de la Política de Seguridad y Privacidad de la Información.
- Acompañar a las dependencias y/o procesos en la identificación y gestión de los riesgos de seguridad de la información, realizando la revisión, análisis y consolidación de la información.
- Definir la Arquitectura de Seguridad de Información en línea con la arquitectura de tecnología de la Entidad.
- Determinar la estrategia de uso y apropiación de la Seguridad de la Información.
- Establecer indicadores de gestión de calidad del Proceso de Seguridad de la Información en la Entidad.
- Asesorar en materia de Seguridad de la Información a la entidad.

8.7. Funcionarios y/o contratistas

Como usuarios que acceden a los sistemas de información de la Entidad para el cumplimiento de sus funciones y obligaciones tienen la responsabilidad de cumplir y aplicar la Política de seguridad y privacidad de la información establecida.

9. Aprobación

ELABORÓ	APROBÓ
Joe Alexander Nuñez Yaguna Profesional Universitario SIS	Diego Alonso Arias Murcia Subdirector de Informática y Sistemas