Control de cambios

Versión	Fecha	Descripción de la modificación
01	13 de febrero de 2020	Se aprueba el Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Secretaría Distrital de Gobierno.
02	16 de febrero del 2021	Se ajusta las metas para la vigencia 2021
03	31 de enero de 2022	Se realiza la actualización del plan de tratamiento de riesgos para la vigencia 2022
04	27 de enero de 2023	Se realiza la actualización del plan de tratamiento de riesgos de seguridad de la información para la vigencia 2023

Método de Elaboración	Revisa	Aprueba
El documento se elabora de acuerdo con las indicaciones de la Oficina Asesora de Planeación y el grupo de trabajo de la Dirección de Tecnología e Información.	**Orlando Benavides Santacruz** Proceso Gerencia de TIC Director de Tecnologías e Información **Angela Patricia Cabeza** Profesional analista de la OAP	**Martha Liliana Soto Iguarán** Líder del Macroproceso Gerencia de la Información Subsecretario de Gestión Institucional **Orlando Benavides Santacruz** Director de Tecnologías e Información El documento fue revisado y aprobado mediante caso en aplicativo Hola No. **292879**

Tabla de contenido

1. INFORMACIÓN GENERAL

1.1 Introducción

En el contexto de la ciberseguridad, hoy día las organizaciones su encuentran en constante riesgo de diferentes ciberamenazas, de tal manera que las organizaciones deben de tener identificados los activos de información críticos, con el fin de dar respuestas a las partes interesadas externas e internas. Por lo anterior, la Secretaria Distrital de Gobierno construye este documento denominado plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, el cual tiene como objetivo dar respuesta a los objetivos estratégicos de la organización y al plan estratégico de tecnologías de la información, donde su desarrollo requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización. Adicionalmente se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

1.2 Propósito

Definir los lineamientos y realizar las actividades necesarias para tratar de manera preventiva e integral los riesgos de Seguridad y Privacidad de la Información a los que la Secretaría Distrital de Gobierno puede estar expuesta para apoyar el cumplimiento del marco estratégico de la Entidad, por medio de la protección de la integridad, confidencialidad y disponibilidad de la información.

1.3 Responsable

El responsable de la Seguridad y Privacidad de la información y el grupo asignado, el cual está bajo las directrices de la Dirección de Tecnologías e Información.

1.4 Glosario [1]

Activo de información: Conocimiento o información que tiene valor para el individuo u organización.

Amenazas: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Confidencialidad: Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

Integridad: Propiedad de exactitud y completitud.

No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital, puede debilitar el logro de los objetivos económicos y sociales, así como afectar la soberanía nacional la integridad territorial, el orden constitucional y los intereses nacionales, incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

1.5 Siglas

DTI: Dirección de Tecnologías e Información
MIPG: Modelo Integrado de Planeación y Gestión

2. ESTRUCTURA DEL PLAN

El presente documento se fundamenta en los propósitos, objetivos generales y específicos establecidos en el documento Manual de Gestión del Riesgo (PLE-PIN-M001), que se base en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital.

[1] Consultoría "Guardianes de la Información". Alta Consejería Distrital de las Tics. http://ticbogota.gov.co/documentos/guardianes-la-informaci%C3%B3n

Contiene también la metodología para el manejo de los riesgos de seguridad y privacidad de la información y la Política de Gestión de riesgo.

2.1 Objetivos

- Brindar lineamientos para la administración de los riesgos de seguridad de la información.
- Identificar, valorar y clasificar los riesgos de seguridad digital de la secretaria Distrital de Gobierno
- Definir las actividades requeridas para la implementar al tratamiento de riesgos de seguridad de la información.
- Evaluar el nivel de riesgo actual con el impacto generado después de implementar el plan de tratamiento de riesgos de seguridad de la información.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad de la información.

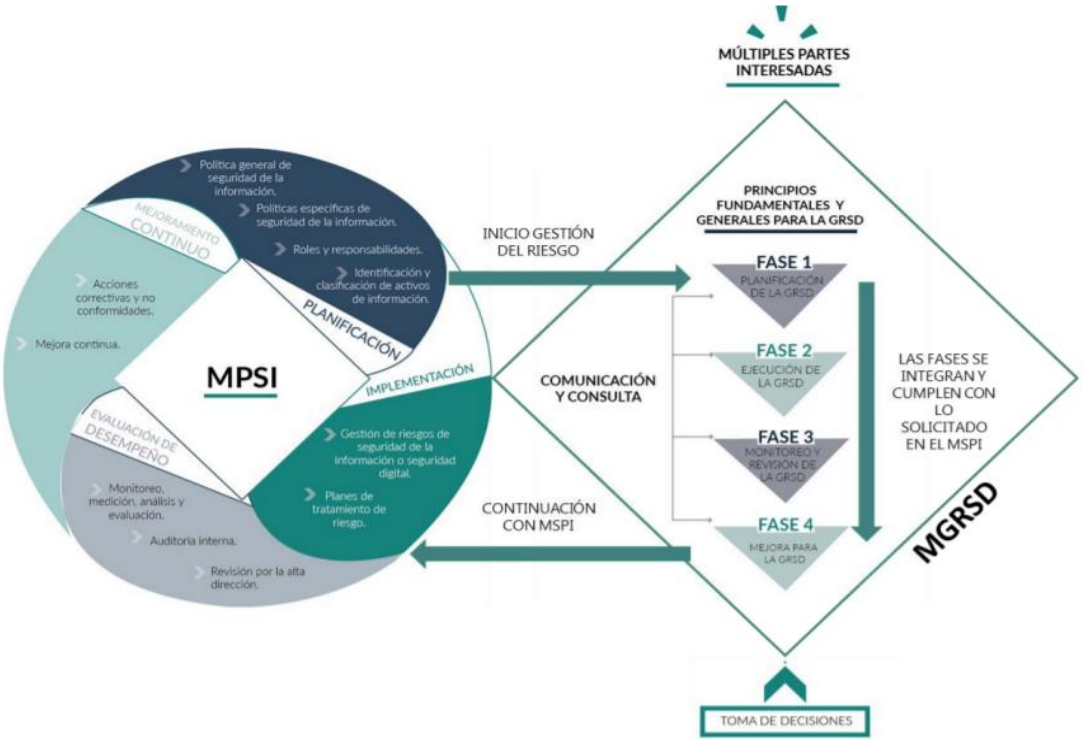
2.2 Alcance

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se identifiquen a **Nivel central y Nivel Local** que se encuentren en los niveles moderado, mayor y catastrófico. Las actividades que se relacionan a continuación se realizarán conforme a los manuales y procedimientos para el tratamiento de los riesgos adoptados por del sistema de gestión de la Entidad en el marco de los lineamientos del MIPG.

2.3 Política de administración del riesgo

La Secretaría de Gobierno se compromete a identificar, analizar, valorar y monitorear los riesgos que impidan el cumplimiento de los objetivos institucionales, con el apoyo de los servidores públicos, contratistas y la participación de la ciudadanía; alcanzando las metas trazadas de manera transparente y eficaz en la gestión de los procesos, la gestión ambiental, seguridad digital y la gestión de seguridad de la información, en pro del mejoramiento continuo de la Entidad.

2.4 Marco Referencial



Fuente: MinTIC [2]

2.5 Desarrollo metodológico

2.5.1 Fase 1 "Planificación"

En esta fase se realizará todas las actividades inherentes con la actualización de los lineamientos de gestión de riesgos y capacitación y sensibilización de los dueños y delegados de proceso, en el cual se comprenden las siguientes actividades:

- Definición del contexto interno, externo y de los procesos de la entidad pública.

[2] Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

2.5.1.1 Contexto interno y externo

La Secretaría Distrital de Gobierno realizará la identificación del contexto interno y externo de la entidad, sin embargo, es necesario profundizar en este análisis relacionado con seguridad digital, por lo tanto, a continuación, se dan unas directrices adicionales para realizar la actividad adecuadamente

2.5.1.1.1 Establecimiento del contexto externo

Para determinar el contexto externo, la Secretaría Distrital de Gobierno debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017.
- Dependencias económicas y financieras por parte de otras empresas.
- Entorno cultural.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.
- Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web. Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, eco económico y ambiental que tengan alguna relación con las operaciones asociadas a la secretaria distrital de gobierno.

2.5.1.1.2 Establecimiento del contexto interno

El contexto interno considera factores que impactan directamente a:

- La secretaria distrital de gobierno, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

2.5.1.1.3 Identificación de activos de seguridad digital

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI que utiliza la organización para su funcionamiento. Es necesario que la secretaria distrital de gobierno identifique los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública. Para la generación de este inventario, la Secretaría Distrital de Gobierno debe tener en cuenta los siguientes pasos:

Fuente: Elaboración propia

2.5.1.1.4 Identificar los riesgos inherentes de seguridad digital

De acuerdo con la metodología de gestión del riesgo de la secretaria distrital de gobierno, para identificar los riesgos de seguridad digital, se deben tener en cuenta los siguientes criterios:

- Afectación a la confidencialidad
- Afectación a la integridad
- Afectación a la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados.

Identificación de Amenazas:

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

Deliberadas (D), fortuito (F), ambientales (A)

EJEMPLOS DE AMENAZAS COMUNES		
Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios de documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A

	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Tabla amenazas comunes
Fuente: ISO 27005:2009

FUENTES DE AMENAZAS HUMANAS		
Fuente de Amenaza	Motivación	Acciones Amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	Piratería
		Ingeniería social
		Intrusión, accesos forzados al sistema
		Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador (por ejemplo, espionaje cibernético)
		Acto fraudulento (por ejemplo, repetición, personificación, interceptación)
		Soborno de la información
		Suplantación de identidad
		Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/terrorismo
		Guerra de la información (warfare)
		Ataques contra el sistema (por ejemplo, negación distribuida del servicio)
		Penetración en el sistema
		Manipulación del sistema
Espionaje industrial	Ventaja competitiva Espionaje económico	Ventaja de defensa
		Ventaja Política

(Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)		Explotación económica
		Hurto de información
		Intrusión en la privacidad personal
		Ingeniería social
		Penetración en el sistema
		Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (por ejemplo, error en el ingreso de los datos, error de programación)	Asalto a un empleado
		Chantaje
		Observar información reservada
		Uso inadecuado del computador
		Fraude y hurto
		Soborno de información
		Ingreso de datos falsos o corruptos
		Interceptación
		Código malicioso (por ejemplo, virus, bomba lógica, troyano)
		Venta de información personal
		Errores en el sistema (bugs)
		Intrusión al sistema
		Sabotaje del sistema
		Acceso no autorizado al sistema

Tabla amenzas dirigidas por el hombre
Fuente: iso 27005:2009

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la secretaria distrital de gobierno debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el dueño del riesgo, es decir, "quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo".

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- Lluvia de ideas: mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la

entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.

- Juicio de expertos: a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad digital se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración

2.5.1.1.5 Identificación y evaluación de controles

De acuerdo con la metodología una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios.

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar la sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA (Tomados del Anexo A de la Norma ISO/IEC 27001:2013) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho anexo.

2.5.1.1.6 Tratamiento de los riesgos de seguridad digital

Una vez se han identificado los riesgos, la secretaria distrital de gobierno debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional. El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, secretaria distrital de gobierno puede tener en cuenta las opciones para tratar el riesgo como son las siguientes:

- Evitar
- Aceptar
- Transferir
- Mitigar

NOTA: Si la secretaria distrital de gobierno decide mitigar o tratar el riesgo mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad digital, sin embargo, la entidad pública puede implementar nuevos controles de seguridad

que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

2.5.2 Fase 2 "Ejecución"

Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la Fase 1.

Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad de la información deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (Primer Línea de Defensa y la Oficina de Tecnologías de la Información -TI generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

2.5.3 Fase 3 "Monitoreo y revisión"

La Secretaría Distrital de Gobierno a través de las Tres Líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Nota: una vez que el plan de tratamiento de riesgos se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad pública debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

2.5.4 Fase 4 "Mejoramiento continuo de la gestión del riesgo de seguridad digital"

La Secretaría Distrital de Gobierno debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse. Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad digital de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano. Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

2.6 Metodología para la gestión del riesgo de seguridad digital en la Secretaría Distrital de Gobierno

Las actividades planteadas para la vigencia 2023

FASE	ACTIVIDAD	TAREA	RESPONSABLE	FECHA INICIO	FECHA FIN
H	Identificación, análisis y evaluación de riesgos de seguridad de la información en Nivel Local	identificación, análisis y evaluación de riesgos de seguridad de la información en Nivel Local	Equipo de seguridad de la información	mar-1	Nov-23
H	Aceptación de los riesgos identificados y los planes de tratamiento para nivel local	Aprobar y publicar la matriz de riesgos de seguridad de la información	Equipo de seguridad de la información	jun-23	Nov-30

H	Realizar seguimiento de implementación de controles a los riesgos identificados para las dependencias de nivel central	Realizar el monitoreo de la adopción de los controles por parte de los dueños de proceso	Equipo de seguridad de la información	mar-23	dic-23
V	Mejoramiento	Identificación de oportunidades en el proceso de gestión del riesgo de seguridad de la información.	Equipo de seguridad de la información	jun-23	nov-23
A	Revisión	Revisión de resultados y reporte de indicadores	Equipo de seguridad de la información	nov-23	dic-23

3. ELEMENTOS ESTRUCTURANTES

3.1 Metas

Para la vigencia 2023 se plantean las siguientes metas

- Realizar la identificación, valoración y clasificación de los riesgos de seguridad de la información de las 20 Alcaldías locales.
- Seguimiento y monitero de los riesgos de seguridad de la información de las 21 dependencias del Nivel Central.

3.2 Indicadores

Indicadores	Variables	Fórmula
Número de alcaldías locales con riesgos de seguridad digital identificados.	1. Mesas de trabajo con las dependencias	**(No de dependencias con riesgos identificados/No dependencias citadas) *100**

Número de dependencias del nivel central con riesgos monitoreados.	2. Mesas de trabajo con las dependencias	**(No de dependencias con riesgos monitoreados/No dependencias citadas) *100**

3.3 Periodo de aplicación del plan

Vigencia 2023

3.4 Periodicidad de medición

Trimestral

3.5 Documentos internos

Código	Documento
PLE-PIN-M001	**Manual de gestión del riesgo**

3.6 Normatividad vigente

Norma	Año	Epígrafe	Artículo(s)
Ley 1341	2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnología e Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones	Toda la norma
CONPES 3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.	Toda la norma
Ley 1581	2012	Disposiciones generales para la protección de datos personales	Toda la norma
Decreto 1078	2015	Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información)	Toda la norma
Decreto 1081	2015	"Decreto Reglamentario Único del Sector Presidencia de la República" (En especial Libro 2)	Toda la norma

Norma	Año	Epígrafe	Artículo(s)
Decreto 415	2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.	Toda la norma
Resolución CDS 004	2017	Fortalecimiento Institucional en Materia de TIC, para Plan Estratégico de Tecnología y Sistemas de Información (PETI) y para la Gestión de Proyectos TIC	Toda la norma
CONPES 3854	2017	Política Nacional de Seguridad Digital	Toda la norma
Decreto 1499	2017	Modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.	Capítulo 2
CONPES 3920	2018	Política Nacional de Explotación de datos.	Toda la norma
Resolución 783	2018	Creación del Comité Institucional de Gestión y Desempeño	Toda la norma
Decreto 1008	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 Tecnología e Información y las Comunicaciones.	Toda la norma
Ley 1978	2019	Moderniza el sector de las Tecnología e Información y las Comunicaciones (TIC), distribuye competencias, crea un regulador único y dicta otras disposiciones.	Articulo 22
Directiva 002	2019	Simplificación de la interacción digital entre los ciudadanos y el estado.	Toda la norma
Generales		**Lineamientos del marco de referencia establecidos por**	

Norma	Año	Epígrafe	Artículo(s)
		MinTIC y que incluyen Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.	

4.3. Documentos externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Ámbitos guardianes de la seguridad	2019	Alta Consejería Distrital de las TICS	http://ticbogota.gov.co/documentos/guardianes-la-informaci%c3%b3n