




 <b>CONCEJO</b> SANTIAGO DE CALI	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			 <b>SISTEMA DE GESTIÓN DE LA CALIDAD</b>
	<b>CÓDIGO: MA.301.23.002</b>	<b>FECHA DE APROBACION: 06-10-2023</b>	<b>VERSIÓN: 001</b>	



**OFICINA INFORMÁTICA**

**ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y  
PRIVACIDAD DE LA INFORMACION (MSPI)**

**SANTIAGO DE CALI, AGOSTO DEL 2021**

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**CONTENIDO**

INTRODUCCIÓN .....3

CONFORMACIÓN DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN .....4

1. Requerimientos Generales de la Norma ISO/IEC 27001:2013 .....4

2. Estructura de la Organización de Seguridad de la Información .....4

3. Comité Institucional de Gestión y Desempeño .....5

    3.1. Integrantes del Comité Institucional de Gestión y Desempeño .....5

    3.2. Funciones del Comité Institucional de Gestión y Desempeño .....5

    3.3. Conocimientos y experiencia del Comité .....6

4. Líder del Modelo de Seguridad y Privacidad de la Información .....7

    4.1. Funciones del Líder del MSPI .....7

    4.2. Conocimientos y experiencia del Líder del MSPI .....9

5. Comité Técnico de Seguridad y Privacidad de la información .....9

    5.1. Funciones del Comité Técnico de Seguridad y Privacidad de la Información. ....9

6. Oficial de Seguridad de la Información .....10

    6.1. Funciones del Oficial de Seguridad de la Información .....11

    6.2. Conocimientos y Experiencia .....13

7. Staff de Seguridad de la Información .....13

    7.1. Funciones del Analista de Seguridad Administrativo .....13

    7.2. Conocimientos y Experiencia .....15

    7.3. Funciones del Analista de Seguridad Técnico .....16

    7.4. Conocimientos y Experiencia .....16

8. Personal de Calidad .....17

    8.1. Funciones del Personal de Calidad .....17

    8.2. Conocimientos y Experiencia .....17

9. Área de Control Interno .....17

    9.1. Funciones del Área de Control Interno .....18

    9.2. Conocimientos y Experiencia del Área de Control Interno .....18

10. Procesos .....18

    10.1. Funciones de los Procesos .....19

    10.2. Funcionarios de Contacto para el modelo de seguridad por proceso .....20

    10.3. Conocimientos y Experiencia .....20

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> <b>MA.301.23.002</b>	<b>FECHA DE APROBACION:</b> <b>06-10-2023</b>	<b>VERSIÓN:</b> 001	



**INTRODUCCIÓN**

El Modelo de Seguridad y Privacidad de la Información (en adelante MSPI), imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), Sé encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación.

Dentro de los estándares internacionales en materia de seguridad de la información se encuentra la Norma ISO/IEC 27001:2013 que define todo lo concerniente a la implementación de un sistema de gestión de seguridad, establece la necesidad de definir y documentar de acuerdo con la política de seguridad de la información, las responsabilidades y roles de las personas que forman parte del sistema.

Dichos roles, se pueden agrupar en tres niveles principales según las funciones y el alcance. Estos niveles son:

- Nivel estratégico, El nivel estratégico toma decisiones alineadas con los objetivos del Concejo Distrital de Cali y elabora las directrices para encaminar la organización en pro de la seguridad de la información. Este nivel está en cabeza del Comité Institucional de Gestión y Desempeño, en el cual se encuentran presentes el jefe de la oficina de Informática y Telemática y el líder del MSPI.
- Nivel táctico, Encargado de unir las decisiones estratégicas del Concejo distrital de Cali, con las labores diarias operativas, de tal manera que se escalen las necesidades operativas al nivel estratégico y se interioricen las decisiones ejecutivas en todas las áreas de la organización. Dicho nivel está en cabeza del Líder del MSPI, el jefe de la oficina de Informática y Telemática y los líderes de proceso que intervienen dentro del alcance del MSPI.
- Nivel operativo, Como su nombre lo indica, este nivel se encarga de todas las labores propias de los procesos habituales de la organización. Ejecuta todas las directrices creadas por los niveles estratégicos y tácticos y está en cabeza del grupo de seguridad de la información, Líder del MSPI, y los líderes de los diferentes procesos del Concejo Distrital de Cali que se encuentran incluidos en el alcance del Modelo de Seguridad y Privacidad de la Información.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**CONFORMACIÓN DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN**

**1. Requerimientos Generales de la Norma ISO/IEC 27001:2013**

Como parte de la definición del Modelo de Seguridad y Privacidad de la Información se recomienda una estructura de seguridad, con el fin de cumplir con lo establecido en la Norma ISO/IEC 27001:2013, en la Cláusula 5: Liderazgo, donde intervienen los numerales 5.1 Liderazgo y Compromiso, 5.2 Política y 5.3 Roles, responsabilidades y autoridades en la organización. Lo anterior se encuentra a lineado con dominio número 6 “Organización de la Seguridad de la Información” del Anexo A, que incluye los siguientes controles:

**Clausula 5. Liderazgo**

**5.1 Liderazgo y Compromiso**

La dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información.

**Anexo A**

**A 6.1 Organización interna**

**A 6.1.1 Roles y responsabilidades para la seguridad de la información.**

Se deben definir y asignar todas las responsabilidades de la seguridad de la información.

**A 6.1.2 Separación de deberes.**

Los deberes y áreas de responsabilidades en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

**2. Estructura de la Organización de Seguridad de la Información**

Como parte integral del Modelo de Seguridad y Privacidad de la Información del Concejo Distrital de Cali es necesario definir una organización de seguridad de la información, la cual estará en cabeza del Comité Institucional de Gestión y Desempeño.

La Organización de Seguridad de la Información estará compuesta por:

- Comité Institucional de Gestión y Desempeño.
- Líder del MSPI
- Comité Técnico de Seguridad y Privacidad de la Información.
- Jefe Oficina de Informática y Telemática.
- Staff de la Oficina de Informática y Telemática
- Procesos incluidos en el alcance del MSPI.
- Proceso de calidad.
- Proceso de control interno.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

A continuación, se describe cada uno de los componentes de la Organización de Seguridad de la Información definidos para el Modelo de Seguridad y Privacidad de la Información.



**3. Comité Institucional de Gestión y Desempeño**  
El Comité el órgano de máxima autoridad y responsabilidad sobre el MSPI, representa el nivel estratégico y de esta forma es responsable por el alineamiento del mismo con los objetivos del Concejo Distrital de Cali.

**3.1. Integrantes del Comité Institucional de Gestión y Desempeño**  
El comité está conformado por los siguientes integrantes:

- Presidente del Concejo.
- Secretario General del Concejo.
- Líder del MSPI.
- Comité Técnico de Seguridad y Privacidad de la Información.
- Oficial de Seguridad de la Información.
- Lideres de Proceso.
- Staff de seguridad de la información.
- Control interno.
- Persona encargada de Calidad.

**3.2. Funciones del Comité Institucional de Gestión y Desempeño**  
Las funciones del comité respecto al Modelo de Seguridad y privacidad de la información son las siguientes:


- Validar y aprobar el alcance y límites del MSPI en términos de las características del negocio, la organización, sus activos, tecnología.
- Validar y aprobar la política del MSPI en términos de las características del negocio, la organización, sus activos y tecnología.
- Validar y aprobar una metodología de valoración del riesgo que sea adecuada para la medición del MSPI del Concejo Distrital de Cali.
- Validar y aprobar los riesgos resultantes luego de efectuar el correspondiente tratamiento sobre estos (Riesgo residuales).
- Validar y autorizar la implementación y operación del MSPI.
- Validar y aprobar la declaración de aplicabilidad propuesta por el líder del MSPI.
- Validar y aprobar un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

- Validar y aprobar la gestión de nuevos recursos para el MSPI para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el MSPI.
- Tener conocimiento de los resultados de las investigaciones realizadas a los incidentes de seguridad de la información.
- Tener conocimiento sobre los resultados de los procedimientos de seguimiento y revisión del MSPI.
- Tener conocimiento sobre revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI, y la revisión de los controles de seguridad) teniendo en cuenta incidentes, medición de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.
- Validar y aprobar los planes de seguridad desarrollados.
- Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.
- Aprobar y Revisar los indicadores del Sistema de Gestión de la Seguridad de la Información.
- Emanar los comunicados a la organización que se refieren a la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua.
- Validar y aprobar criterios para aceptación de riesgos, y los niveles de riesgo aceptables.
- Tener conocimiento de la asignación de responsabilidades definidas en el MSPI; para que todo el personal presente las competencias suficientes en la realización de las tareas encomendadas.
- Aprobar y revisar el alcance, objetivos y estrategias del Modelo de Seguridad y Privacidad de la Información.
- Aprobar y revisar periódicamente las políticas y normas de seguridad de la información.

**3.3. Conocimientos y experiencia del Comité**  
**Conocimientos mínimos.**

- Conocimientos Básicos en modelos de Seguridad y Privacidad de la Información.
- Conocimientos Básicos en directrices de Gobierno Digital y disposiciones legales en materia de Seguridad de la Información.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**4. Líder del Modelo de Seguridad y Privacidad de la Información**

El Líder del MSPI, permite la integración entre los aspectos estratégicos y tácticos que se presenten en el MSPI.


Es el representante del MSPI ante el Comité Institucional de Gestión y Desempeño y participa en la toma de decisiones.

**4.1. Funciones del Líder del MSPI**

- Validar y proponer al comité el alcance y límites del MSPI en términos de las características del negocio, la organización, sus activos, tecnología.
- Validar y proponer al comité la política del MSPI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología.
- Validar y proponer al comité una metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.
- Validar y proponer al comité una metodología de valoración del riesgo que sea adecuada al MSPI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, que se hayan identificado.
- Conocer la gestión de identificación de riesgos realizada por los procesos.
- Coordinar aspectos relacionados con la gestión de riesgos, así:
  - Análisis y evaluación de riesgos.
  - Identificación y evaluación de opciones para tratamiento de riesgos.
  - Selección de objetivos de control y controles para el tratamiento de riesgos.
- Validar y presentar al comité los riesgos residuales propuestos por las áreas.
- Validar la implementación y operación del MSPI.
- Validar y presentar al comité la declaración de aplicabilidad.
- Validar la implementación del plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.
- Validar la implementación de controles seleccionados para cumplir con los objetivos.
- Validar la definición de la eficacia de los controles o grupos de controles seleccionados a implementar.
- Conocer y validar la implementación de programas de formación y toma de conciencia relacionados con el MSPI.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> <b>MA.301.23.002</b>	<b>FECHA DE APROBACION:</b> <b>06-10-2023</b>	<b>VERSIÓN:</b> 001	

- Validar en el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Conocer los procedimientos de seguimiento y revisión del MSPI.
- Conocer la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Conocer la revisión a las valoraciones de los riesgos a intervalos planificados, así mismo el nivel de riesgo residual y riesgo aceptable identificado.
- Conocer la realización y el resultado de auditorías internas al MSPI.
- Conocer las revisiones regulares a la eficacia del MSPI (que incluyen el cumplimiento de los controles de seguridad, la política y objetivos del MSPI) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Validar y presentar al comité los planes de seguridad desarrollados.
- Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.
- Validar la documentación del MSPI, desarrollada por el Oficial de Seguridad.
- Validar el procedimiento para definir las acciones de gestión documental desarrolladas por el Oficial de seguridad.
- Validar que se cumpla el establecimiento y mantenimiento de registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del MSPI.
- Validar y presentar al comité los criterios para aceptación de riesgos y los niveles de riesgo aceptables.
- Recomendar al Comité Institucional de Gestión y Desempeño, sobre posibles actualizaciones de políticas, normas y estándares de Seguridad de la Información.
- Liderar la realización de análisis e investigaciones sobre los incidentes de seguridad de la información.
- Liderar la realización de la gestión de activos de información y riegos por parte de la empresa.
- Velar por una permanente integración del Sistema de Gestión de Seguridad de la Información con el Sistema de Gestión de Calidad.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**4.2. Conocimientos y experiencia del Líder del MSPI**

El líder del MSPI debe contar con experiencia el diseño e implementación de Sistemas de Gestión de Seguridad de la Información.

**Conocimientos Mínimos**

- Conocimientos en Sistemas de Gestión de la Seguridad de la Información.
- Conocimientos sobre modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).
- Experiencia en el diseño e implementación de sistemas de gestión de seguridad de la información.
- Conocimiento sobre la Legislación relacionada con Seguridad de la Información.
- Conocimiento en el diseño de controles.
- Conocimientos en el análisis de riesgos.

**Conocimientos Deseados**

- Conocimiento sobre estrategias de Seguridad de la Información.
- Participación en cursos de formación en Seguridad de la Información y continuidad del negocio.

**5. Comité Técnico de Seguridad y Privacidad de la información**

El comité técnico de seguridad y privacidad de la información apoya al oficial de seguridad en las decisiones sobre la definición de políticas de dominio, normas, metodologías, planes de sensibilización y otros aspectos que impacten a una gran parte de la organización.

La existencia del comité técnico, ya que está conformado por diferentes roles de la organización, garantiza la interdisciplinaridad y el cumplimiento de las exigencias del negocio y sus objetivos.

Los integrantes que hacen parte del comité de seguridad y privacidad de la información son:

- Oficial de Seguridad de la Información.
- Staff de seguridad de la información.
- Funcionario del Sistema de Gestión de calidad.
- Funcionario de control interno.
- Funcionario del área jurídica.
- Funcionarios de las unidades estratégicas del negocio.
- Funcionarios de los procesos que se encuentren involucrados dentro del alcance del MSPI.

**5.1. Funciones del Comité Técnico de Seguridad y Privacidad de la Información.**

- Participar en la definición y revisión del alcance y límites del MSPI en términos de las características del negocio, la organización, sus activos, tecnología.


	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

- Participar en la definición y revisión de la política del MSPI en términos de las características del negocio, la organización, sus activos y tecnología.
- Participar en la definición y revisión de la metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.
- Participar en la definición y revisión de una metodología de valoración del riesgo que sea adecuada para el MSPI y la revisión de los requisitos reglamentarios, legales y de seguridad de la información del negocio aplicables al Concejo Distrital de Cali.
- Participar en la definición y revisión del proceso de atención de incidentes.
- Validar el plan de tratamiento de riesgos presentado por los procesos incluidos en el alcance del MSPI.
- Participar en el diseño de programas de formación y toma de conciencia relacionados con el MSPI.
- Validar la necesidad de nuevos recursos para el MSPI para establecer, implementar, operar, revisar, mantener, mejorar Y hacer seguimiento al MSPI y presentarla al líder del MSPI.
- Validar los procedimientos y controles para prevenir, detectar y dar respuesta oportuna a los incidentes de seguridad.
- Participar en la definición y revisión de los criterios para la aceptación de los riesgos y el nivel de riesgo aceptable.
- Asegurar la realización de revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Validar, cuando se requiera, las acciones correctivas y preventivas propuestas por los procesos.
- Velar por la integración del MSPI con el Sistema de Gestión de Calidad y otros existentes.

**6. Oficial de Seguridad de la Información**



El Oficial de seguridad de la información es el rol encargado de coordinar la ejecución de las actividades derivadas de la planeación, implementación, revisión y mantenimiento del MSPI. Coordina el aspecto táctico y operativo ejecutando las directrices del comité técnico de seguridad y privacidad de la información y líder del MSPI.

El Oficial de seguridad se apoya en el comité técnico para definición de metodologías, procedimientos y planes de seguridad de la información con el objeto de tener en cuenta las necesidades del negocio, sus procesos y determinar la mejor opción con el menor impacto para la organización.


	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**6.1. Funciones del Oficial de Seguridad de la Información**

- Definir y proponer al líder del MSPI el alcance y límites del MSPI en términos de las características del negocio, la organización, sus activos, tecnología.
- Definir y proponer al líder del MSPI la política de MSPI en términos de las características del negocio, la organización, sus activos y tecnología.
- Definir y proponer al líder de seguridad la metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.
- Definir y proponer al líder de seguridad una metodología de valoración del riesgo que sea adecuada al MSPI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio que se han identificado.
- Coordinar la realización de la gestión de identificación de riesgos a realizar por los procesos incluidos en el alcance del MSPI.
- Coordinar la realización de la gestión de riesgos que incluye:
  - Análisis y evaluación de riesgos.
  - Identificación y evaluación de opciones para tratamiento de riesgos.
  - Selección de objetivos de control y controles para el tratamiento de riesgos de acuerdo al anexo A de la norma ISO 27001.
- Recibir de las áreas responsables los riesgos residuales y presentarlos al líder del MSPI.
- Validar la implementación y operación del MSPI.
- Definir y presentar al líder del MSPI una declaración de aplicabilidad.
- Consolidar la información sobre el plan de tratamiento de riesgos diseñado por las áreas responsables y presentarlo al líder del MSPI.
- Coordinar la implementación del plan de tratamiento de riesgos de cada una de las áreas.
- Coordinar la implementación de controles seleccionados de cada área.
- Coordinar la definición de la eficacia de los controles o grupos de controles seleccionados por las áreas.
- Coordinar y participar en el diseño de la implementación de programas de formación y toma de conciencia relacionados con el MSPI.
- Validar la necesidad de nuevos recursos para el MSPI para establecer, implementar, operar, revisar, mantener, mejorar Y hacer seguimiento al MSPI y presentarlo al líder del MSPI.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

- Participar en el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Coordinar la realización de los procedimientos de seguimiento y revisión del MSPI.
- Coordinar la realización de la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Coordinar la realización de la revisión de las valoraciones de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable identificado.
- Coordinar la realización de auditorías internas al MSPI en los tiempos que se programen.
- Consolidar la información de las áreas sobre los planes de seguridad desarrollados y presentarla al líder del MSPI.
- Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.
- Gestionar la documentación del MSPI en coordinación con el área encargada de esta labor (Área de Calidad).
- Gestionar el procedimiento para definir las acciones de gestión documental en coordinación con el área de calidad.
- Definir y proponer al líder del MSPI los criterios para aceptación de riesgos y los niveles de riesgo aceptables.
- Coordinar y participar en el diseño del procedimiento de asignación de responsabilidades definidas en el MSPI; para que todo el personal sea competente para realizar las tareas exigidas.
- Coordinar la realización de revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Liderar la realización de análisis e investigaciones sobre los incidentes de seguridad de la información.
- Liderar la realización de la gestión de activos de información y riegos por parte de la empresa.
- Plantear acciones preventivas o correctivas, comunicar al área responsable y validar las acciones propuestas por las áreas.
- Velar por la integración del MSPI con el Sistema de Gestión de Calidad.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

- Liderar el staff de seguridad de la información.

**6.2. Conocimientos y Experiencia**  
**Conocimientos Mínimos**

- Conocimientos avanzados en Modelos de Seguridad y Privacidad de la Información.
- Conocimientos y/o experiencia en la definición de planes estratégicos de seguridad de la información.
- Conocimientos y/o experiencia en la definición de planes de tratamiento de riesgos.
- Modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).
- Conocimiento en problemas de seguridad bases de datos, sistemas operativos, aplicaciones, redes.

**Conocimientos Deseados**

- Ser Auditor Líder ISO/IEC 27001:2013.
- Experiencia en desarrollo y administración de Modelos de Seguridad de la Información.
- Experiencia en el desarrollo de auditorías.
- Conocimiento de estrategias de Seguridad de la Información.
- Cursos y certificaciones relacionadas con Seguridad de la Información, como:
  - Certified Information Systems Security Professional, CISSP.
  - Certified Information Security Management, CISM.
  - Certified Information Systems Auditor, CISA.
  - Certified Ethical Hacker, CEH.

**7. Staff de Seguridad de la Información**

El staff de seguridad de la información, cuyo líder es el oficial de seguridad de la información, es deseable que este conformado por un analista de seguridad administrativa y un analista de seguridad técnica.

Los analistas reportarán al oficial de seguridad de la información y serán su apoyo para el desarrollo de las actividades concernientes al modelo de seguridad en general.



**7.1. Funciones del Analista de Seguridad Administrativo**

Dentro de sus se encuentran la administración y coordinación de las actividades del MSPI, como lo son: la gestión de activos de información, la gestión de riesgos, la medición de indicadores de gestión, entre otras. Las funciones del analista de seguridad administrativo son las siguientes:

- Participar en la definición del alcance y límites del MSPI.
- Participar en la definición de la metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

- Guiar metodológicamente la realización de la gestión de activos de información y tratamiento de los mismos por parte de los procesos del Concejo Distrital de Cali.
- Guiar metodológicamente la realización de la gestión de identificación de riesgos a realizar por los procesos incluidos en el alcance del MSPI.
- Guiar metodológicamente la realización de la gestión de riesgos que incluye:
  - Análisis y evaluación de riesgos.
  - Identificación y evaluación de opciones para tratamiento de riesgos.
  - Selección de objetivos de control y controles para el tratamiento de riesgos.
- Recibir de las áreas responsables los riesgos residuales, consolidarlos y producir información para análisis.
- Guiar metodológicamente a los procesos del Concejo Distrital de Cali en la definición de controles con el objetivo de mitigar los riesgos existentes.
- Preparar la declaración de aplicabilidad.
- Consolidar la información sobre el plan de tratamiento de riesgos diseñado por las áreas responsables.
- Guiar metodológicamente la implementación del plan de tratamiento de riesgos de cada una de las áreas.
- Guiar metodológicamente la implementación de controles seleccionados de cada área.
- Guiar metodológicamente la definición y medición de la eficacia de los controles o grupos de controles seleccionados por las áreas.
- Participar en el diseño de la implementación de programas de formación y toma de conciencia relacionados con el MSPI.
- Participar en el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Coordinar la realización de los procedimientos de seguimiento y revisión del MSPI.
- Participar en la coordinación de la revisión de la valoración de los riesgos, el nivel de riesgo residual y aceptable determinado.
- Participar en la coordinación de la realización de auditorías internas al MSPI en los intervalos planificados.
- Consolidar la información de las áreas sobre los planes de seguridad desarrollados y generar

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

información para análisis.

- Gestionar la documentación del MSPI en coordinación con el área encargada de esta labor (Área de Calidad).
- Participar en el diseño del procedimiento de asignación de responsabilidades definidas en el MSPI; a fin de que todo el personal cuente con las competencias para realizar las tareas exigidas.
- Coordinar la realización de revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Participar en el análisis e investigaciones sobre los incidentes de seguridad de la información.
- Plantear acciones preventivas o correctivas, comunicar al área responsable y validar las acciones propuestas por las áreas.
- Propender por la integración del Sistema de Gestión de Seguridad de la Información con el Sistema de Gestión de Calidad.
- Guiar metodológicamente a los procesos del Concejo Distrital de Cali para la definición de controles con el objetivo de mitigar los riesgos existentes.

**7.2. Conocimientos y Experiencia**  
**Conocimientos Mínimos**

- Conocimientos avanzados en Sistemas de Gestión de la Seguridad de la Información.
- Conocimientos en modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).
- Conocimientos en sistemas de gestión de calidad ISO 9001.

**Conocimientos Deseados**

- Ser Auditor Líder ISO/IEC 27001:2013.
- Experiencia en desarrollo y administración de Modelos de Seguridad de la Información.
- Experiencia en el desarrollo de auditorías.
- Conocimiento de estrategias de Seguridad de la Información.
- Cursos y certificaciones relacionadas con Seguridad de la Información, como:
  - Certified Information Systems Security Professional, CISSP.
  - Certified Information Security Management, CISM.
  - Certified Information Systems Auditor, CISA.
  - Certified Ethical Hacker, CEH.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**7.3. Funciones del Analista de Seguridad Técnico**

Dentro de las funciones del analista se encuentran la gestión de la plataforma de seguridad informática de la Oficina de Informática y Telemática del Concejo, y ser un apoyo constante en la implementación y mejoramiento de la arquitectura de seguridad recomendada. Este analista se enfoca a labores que apoyan el pilar técnico dentro del MSPI. Las funciones del analista de seguridad técnico son las siguientes:

- Soportar y desarrollar los procedimientos que relacionan la utilización de la infraestructura tecnológica: Procedimiento de evaluación de plataforma tecnológica, procedimiento de conexión de equipos, procedimiento para gestión de usuarios.
- Configurar y mantener activos informáticos relacionados con la seguridad de la plataforma. Equipos como firewall (de perímetro externo como interno), Sistemas de Prevención de Intrusos (IPS internet, WAN y granja de servidores), enrutadores, sistemas de gestión y monitoreo; los anteriores dado el caso en el que el Concejo Distrital de Cali cuente con ellos.
- Ser participe en la realización de auditorías sobre configuraciones realizadas en la plataforma de tecnología.
- Guiar la implementación de los controles a nivel tecnológico definidos en el plan de tratamiento de riesgos.
- Participar activamente en el ciclo de vida de gestión de incidentes de seguridad de la información.
- Participar en el proceso de gestión del cambio junto con los administradores de infraestructura si se requieren realizar ajustes de seguridad que pudieran impactar las operaciones al interior del departamento.

**7.4. Conocimientos y Experiencia**  
**Conocimientos Mínimos**

- Conocimientos en Sistemas de Gestión de la Seguridad de la Información.
- Conocimientos en modelos de Gestión de Incidentes de Seguridad y Análisis Forense.
- Conocimiento en el desarrollo de procedimientos de infraestructura tecnológica.
- Problemas de seguridad asociados a: Servidores, bases de datos, aplicaciones.
- Conocimiento de seguridad en: Bases de datos, sistemas operativos, aplicaciones, redes.
- Conocimiento en tecnologías de seguridad: Firewalls, IDS/IPS, antivirus, sistemas biométricos.

**Conocimientos Deseados**

- Ser Ethical Hacker Certificado (CEH)
- Cursos y certificaciones relacionadas con soluciones de seguridad informática
- Experiencia en el desarrollo de auditorías.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**8. Personal de Calidad**

Actualmente el Concejo Distrital de Cali no cuenta dentro de su organigrama organizacional con un área de calidad, más cuenta con personal que se encarga de la administración del Sistema de Calidad dentro del Concejo Distrital de Cali, en coordinación con el oficial de seguridad de la información, estará encargada de la gestión documental del MSPI integrándolo con el Sistema de Gestión de Calidad.

**8.1. Funciones del Personal de Calidad**

Dentro de las funciones del personal de calidad son las siguientes:

- Gestionar la documentación del MSPI, de tal manera que esté alineada con los demás sistemas de gestión existentes.
- Mantener actualizada y publicada toda la documentación relacionada con el MSPI. Esta función debe realizarse en coordinación con el Oficial de Seguridad de la Información.
- Revisar continuamente los documentos del MSPI, para mantenerlos alineados con las normas y reglamentaciones vigentes respecto a la gestión documental.
- Garantizar, desde el punto de vista documental, la integración del Modelo de Seguridad y Privacidad de la Información con el Sistema de Gestión de Calidad.
- Participar en la definición de la metodología de valoración del riesgo, velando por su integración con las demás metodologías de riesgos existentes.

**8.2. Conocimientos y Experiencia**

**Conocimientos Mínimos**

- Conocimientos en el manejo de Sistemas de Calidad Implementados bajo la norma ISO 9001

**Conocimientos Deseables**

- Conocimiento en Sistemas de Gestión de Seguridad de la Información.
- Experiencia certificada en el manejo de Modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).
- Conocimiento de Modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).

**9. Área de Control Interno**

A diferencia del numeral anterior, el Concejo Distrital de Cali cuenta con un área de control interno y se hace necesario alinear sus funciones teniendo en cuenta el nuevo sistema de gestión de seguridad de la información. Ésta estará encargada de gestionar las auditorías internas y externas al Sistema de Gestión de Seguridad de la Información.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**9.1. Funciones del Área de Control Interno**

- Revisar periódicamente en coordinación con el oficial de seguridad y el área de calidad, los procedimientos de seguimiento y revisión del MSPI.
- Realizar en coordinación con el oficial de seguridad, revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Realizar en coordinación con el oficial de seguridad las auditorías internas al MSPI.
- Presentar informes de auditoría al Líder del MSPI o comité de seguridad y Privacidad de la información.
- Determinar, en forma conjunta con el Oficial de Seguridad de la Información la efectividad de las soluciones de las no conformidades presentadas por los procesos.
- Velar por la integración del Sistema de Gestión de Seguridad de la Información con el Sistema de Gestión de Calidad, particularmente en la planeación y ejecución de auditorías.

**9.2. Conocimientos y Experiencia del Área de Control Interno**  
**Conocimientos Mínimos**


- Sistemas de Gestión de la Seguridad de la Información.
- Cocimientos en gestión de activos de información.
- Experiencia en desarrollo de auditoría de seguridad de la información.
- Conocimiento en Gestión de Riesgos (análisis y control).

**Conocimientos Deseables**

- Ser Auditor Líder ISO/IEC 27001:2013.
- Experiencia certificada en la ejecución de pruebas de vulnerabilidad y Ethical Hacking.
- Experiencia en el manejo de Modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).
- Experiencia en auditoría de sistemas.
- Conocimiento de metodologías de pruebas de vulnerabilidad y Ethical Hacking.
- Conocimiento en el manejo de incidentes de seguridad.


**10. Procesos**

Los procesos de la entidad son responsables por ejecutar el modelo de seguridad y privacidad de la información definido por el comité de seguridad de la información.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

**10.1. Funciones de los Procesos**

- Cumplir con las disposiciones de la política de MSPI en términos de las características del negocio, la organización, sus activos y tecnología.
- Acatar la metodología de identificación, valoración, clasificación y tratamiento de los activos de información.
- Acatar la metodología de valoración del riesgo definida para el MSPI y los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados.
- Realizar la gestión de identificación de riesgos.
- Realizar la gestión de riesgos que incluye:
  - Análisis y evaluación de riesgos.
  - Identificación y evaluación de opciones para tratamiento de riesgos.
  - Selección de objetivos de control y controles para el tratamiento de riesgos.
- Calcular los riesgos residuales y presentarlos al oficial de seguridad de la información.
- Validar la implementación y operación del MSPI.
- Diseñar el plan de tratamiento de riesgos y presentarlo al oficial de seguridad de la información.
- Implementar el plan de tratamiento de riesgos correspondiente.
- Implementar los controles seleccionados.
- Definir la eficacia de los controles o grupos de controles seleccionados.
- Acudir y participar de los programas de formación y toma de conciencia relacionados con el MSPI.
- Implementar los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Ejecutar las recomendaciones derivadas de los procedimientos deseguimiento y revisión del MSPI.
- Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Realizar la revisión de las valoraciones de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable identificado.

	<b>ESTRUCTURA ORGANIZACIONAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI</b>			
	<b>CÓDIGO:</b> MA.301.23.002	<b>FECHA DE APROBACION:</b> 06-10-2023	<b>VERSIÓN:</b> 001	

- Ejecutar las recomendaciones derivadas de las auditorías internas realizadas al MSPI.
- Generar la documentación respectiva a sus responsabilidades que tenga que ver con el MSPI.
- Plantear acciones preventivas o correctivas, comunicar al Oficial de seguridad de la información sobre su efectividad y ejecutar las recomendaciones correspondientes.

**10.2. Funcionarios de Contacto para el modelo de seguridad por proceso**

El rol de contacto para el modelo de seguridad y privacidad de la información tiene la función de enlace entre su proceso y el MSPI. Este rol debe ser seleccionado por el proceso y trabajará de manera coordinada con el personal a cargo de la administración del MSPI.

Dentro de las funciones del rol de contacto se encuentran:

- Ser la persona que facilite, apoye y monitoree el proceso de cambio en su proceso generando conciencia de la importancia de la seguridad en la información y motivando acciones acordes que permitan el éxito de la implementación de los Sistemas de Gestión.
- Velar por la ejecución y ser fuente de consulta de primer nivel del proceso para la identificación, clasificación y tratamiento adecuado de los activos de información.
- Ser fuente de consulta de primer nivel para las inquietudes del proceso sobre la metodología de valoración del riesgo.
- Ser contacto para la coordinación de las diversas actividades del programa de capacitación y sensibilización del Sistema de Gestión.
- Apoyar activamente el monitoreo y medición de resultados de las campañas de sensibilización y capacitación realizadas.
- Plantear acciones preventivas o correctivas y comunicar al Oficial de seguridad sobre su efectividad y ejecutar las recomendaciones correspondientes.

**10.3. Conocimientos y Experiencia**

**Conocimientos Deseados**

- Sistemas de Gestión de la Seguridad de la Información.
- Cocimientos en gestión de activos de información de acuerdo a la metodología definida.
- Conocimientos en gestión de riesgos (análisis y control), de acuerdo a la metodología definida.
- Conocimiento en problemas de seguridad de la información.