CONCEJO
SANTIAGO DE CALI

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONCEJO DE CALI

Descripción breve

Este documento tiene por objetivo trazar y planificar la manera como el Concejo de Santiago de Cali realizará la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital.

OFICINA DE INFORMATICA Y TELEMATICA DEL CONCEJO DE SANTIAGO DE CALI

CONCEJO
SANTIAGO DE CALI

Contenido

CONCEJO
SANTIAGO DE CALI

INTRODUCCIÓN

OBJETIVO

Establecer las acciones necesarias que aseguren la implementación del Modelo de Seguridad y Privacidad de la Información de acuerdo a la política de Gobierno Digital en el Concejo del Municipio de Santiago de Cali bajo el enfoque de mejora continua.

OBJETIVOS ESPECIFICOS

- Identificar las actividades necesarias para garantizar la implementación del MSPI de acuerdo a la Política de Gobierno Digital.
- Estableces un cronograma de trabajo para la implementación del MSPI de acuerdo a las fases recomendadas en el Modelo de seguridad y privacidad de la información.

ALCANCE

El plan contempla las acciones necesarias para la implementación del Modelo de Seguridad y Privacidad de la Información a los procesos y locaciones físicas del Concejo del Municipio de Santiago de Cali.

CONCEJO
SANTIAGO DE CALI

MARCO LEGAL

- Constitución Política. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.

- Ley 527 de 1999. “Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”

- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;”

- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”

- Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países

- Ley 1273 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”. Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418. Revelación de Secreto; Art. 419. Utilización de asunto sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.

- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.

- Ley 1437 de 2011. “Procedimiento Administrativo y aplicación de criterios de seguridad”.

- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”.

- Decreto Ley 019 de 2012. “Racionalización de trámites a través de medios electrónicos.

- Ley 1621 de 2013. “Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones”.

- Decreto 1078 de 2015, por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de Información y las Comunicaciones

- Decreto 1008 de 2018. “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector Tecnologías de la Información y las Comunicaciones”

- Decreto 1413 de 2017. “Por la cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2018, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- Decreto 415 de 2016. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2011 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones”

- Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad digital. CONPES Bigdata

GLOSARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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 una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Habilitador Transversal de Seguridad de la información, como habilitador transversal de la política de Gobierno en digital, permite alinearse a los 2 componentes de la Política de Gobierno digital que son TIC para el estado y TIC pata la sociedad al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la

información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

El Habilitador Transversal de Seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos

sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información - MSPI.

El modelo de seguridad y privacidad de la información entregada por el ministerio de las TIC dentro del marco de la política de Gobierno Digital contempla un ciclo de operación que consta de cinco (5) fases, las cuales permitirán que el Concejo del Municipio de Santiago de Cali pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información.

A continuación se especifican las fases y los productos a desarrollar para la implementación del MSPI en el Concejo del Municipio de Santiago de Cali:

FASE DE DIAGNÓSTICO

En esta fase se pretende identificar el estado actual del Concejo de Santiago de Cali con respecto a los requerimientos del MSPI.

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del Concejo de Santiago de Cali.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

Para realizar esta fase se debe efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico.

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación.

Herramienta: Herramienta de diagnóstico
https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

Producto: Herramienta de diagnóstico diligenciada.

FASE DE PLANIFICACIÓN

En esta fase se debe modificar este plan de seguridad y privacidad de la información manteniendo alineado con el objetivo misional del Concejo de Santiago de Cali, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

A continuación se explica de manera general los productos esperados en la fase de planificación del Modelo de Seguridad y Privacidad de la Información

Política de seguridad y privacidad de la información.

Actualizar la Política de Seguridad y Privacidad de la información contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección del Concejo de Santiago de Cali para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información la cual será divulgada al interior del Concejo.

Políticas Operativas de Seguridad y Privacidad de la Información.

Desarrollar un Manual de políticas a nivel operativo, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior del Concejo de Santiago de Cali; definiendo

las responsabilidades generales y específicas para la gestión de la seguridad de la información.

Procedimientos de Seguridad de la Información.

Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información.

Para desarrollar esta actividad, la Guía No 3 del MSPI- describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior del Concejo de Santiago de Cali.

Guia3: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Roles y Responsabilidades de Seguridad y Privacidad de la Información.

El Concejo de Santiago de Cali debe definirá mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos en el Concejo.

Inventario de activos de información.

Desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

La Guía No 5 del MSPI - Gestión De Activos, brinda información relacionada para poder llevar a cabo esta actividad.

Guía 5. https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Identificación, Valoración Y Tratamiento de Riesgos.

El concejo de Santiago de Cali cuenta con una política de gestión de riesgos la cual debe ser adaptada para que permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información, así como la declaración de aplicabilidad.

En esta actividad lo que se desarrollará es una modificación a la política de riesgos para que considere también los riesgos de seguridad de la información y pueda ser usada la metodología ya definida para identificar y valorar los riesgos de seguridad de la información.

Plan de tratamiento de riesgos

La metodología definida en la política de riesgos será aplicada para la identificación, valoración y tratamiento de riesgos de los activos de información relacionados a seguridad de la información una vez tengamos identificados y clasificados todos los activos de información del Concejo de Santiago de Cali.

Una vez se tengan identificados los riesgos, se identificaran los controles de acuerdo a la Guía No 8 - Controles de Seguridad del MSPI que mitigarán los riesgos identificados y se procede a realizar el plan de tratamiento de riesgos y la declaración de aplicabilidad

Guía 8. https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Plan de Comunicaciones.

Definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del Concejo de Santiago de Cali.

Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad.

Para estructurar dicho plan puede utilizar la Guía No 14 del MSPI – plan de comunicación, sensibilización y capacitación.

Guía 14. https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Plan de transición de IPv4 a IPv6.

Desarrollar el diagnóstico de IpV4 a IpV6 y el plan para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, apoyados en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

FASE DE IMPLEMENTACIÓN

Esta fase llevar acabo la implementación de la planificación realizada en la fase de planificación y se hace importante énfasis en la implementación de los controles que mitigan los riesgos, es decir el plan de mitigación de riesgos.

A continuación se explica de manera general los productos esperados en la fase de Implementación del Modelo de Seguridad y Privacidad de la Información en el Concejo de Santiago de Cali.

Implementación del plan de tratamiento de riesgos.

Desarrollar Informes de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. Es decir del estado de implementación y efectividad de los controles escogidos para la mitigación de cada riesgo identificado en los activos de información.

Indicadores De Gestión.

Definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

FASE DE EVALUACIÓN DE DESEMPEÑO

En esta fase, la oficina de control interno debe desarrollar dentro del proceso de auditorías, debe planificar y desarrollar auditorias para el seguimiento y monitoreo del MSPI

A continuación se explica de manera general los productos esperados en la fase de Evaluación de desempeño del Modelo de Seguridad y Privacidad de la Información en el Concejo de Santiago de Cali

Plan de Ejecución de Auditorias

El Concejo de Santiago de Cali desarrollará un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Se debe llevar a cabo auditorías y revisiones a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

FASE DE MEJORA CONTINUA

En esta fase el Concejo de Santiago de Cali debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

A continuación se explica de manera general los productos esperados en la fase de Evaluación de desempeño del Modelo de Seguridad y Privacidad de la Información en el Concejo de Santiago de Cali

Plan de mejoramiento

Definir y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño

CONCEJO
SANTIAGO DE CALI

Plan de implementación

No	ACTIVIDADES	TAREAS	MESES												PRODUCTOS (BIENES O SERVICIOS) ENTREGADOS	RESPONSABLES
			1	2	3	4	5	6	7	8	9	10	11	12		
FASE DE DIAGNOSTICO																
1	Realizar el Diagnostico del estado actual de MSPI en el Concejo de Santiago de Cali	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del Concejo de Santiago de Cali.													Herramienta de diganostico Instrumento de Evaluación MSPI completamente diligenciada y con informe de estado de madurez actual	Oficina de Informática y Telemática
		Realizar el diagnóstico de estado actual de IpV4 a IpV6														
FASE DE PLANIFICACIÓN																
2	Realizar el diseño y Planificacion del MSPI	Actualizar la Política de Seguridad y Privacidad de la información													Politica general de seguridad de la información	Oficina de Informática y Telemática
		Desarrollar las Políticas Operativas de Seguridad de la infomracion que sugiere la Guía 2 - Política General MSPI v1													Politicas operativas de	Oficina de Informática y

CONCEJO
SANTIAGO DE CALI

			seguridad de la información	Telemática
		Desarrollar Procedimientos de Seguridad de la Información que sugiere la Guía 3 - Procedimiento de Seguridad de la Información	Procedimientos desarrollados	Oficina de Informática y Telemática
		Acto adminsitrativo definiendo Roles y Responsabilidades de Seguridad y Privacidad de la Información	Acto adminsitrativo desarrollado y propuesto	Oficina de Informática y Telemática
		Desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información como sugiere la La Guía No 5 del MSPI - Gestión De Activos	Metodologia definida	Oficina de Informática y Telemática
		Levantar activos de información	Activos identificados	Oficina de Informática y Telemática
		Modificación a la política de riesgos para que considere también los riesgos de seguridad de la información	Propuesta de Politica de riesgos con cambios sugeridos	Oficina de Informática y Telemática
		Aplicar la politica de riesgos a los activos de informacion identificados y los respectivos controles que mitigan el riesgo	Plan de tratamiento de riesgos	Oficina de Informática y Telemática
		Definir un Plan de comunicación, sensibilización y capacitación en seguridad de la información.	Plan desarollado	Oficina de Informática y Telemática