MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN PESI

TABLA DE CONTENIDO

INTRODUCCIÓN

El concepto de seguridad de la información, según ISO/IEC 27001:2013, radica en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de Gestión de Riesgo, (ISO/ IEC 27001 VERSION 2013, 2013), para lo cual, el plan busca dar respuesta a las exigencias que el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, (MinTic), presenta para todas entidades públicas.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse a los siguientes componentes:

- TIC para la Gestión 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.

- TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

- TIC para Gobierno Abierto que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

El Plan de Seguridad de la Información (PSI), es un documento quetiene por objetivo trazar y planificar la manera como la entidad realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Este plan hace parte del Sistema de Gestión de Seguridad de la Información (SGSI) el cual es una herramienta de la que se dispone para dirigir y controlar la seguridad de la información.

Este documento indica y define plazos anuales, cuáles serán las labores que realizará la entidad con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la entidad.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Las actividades para la administración y la seguridad informática pueden clasificarse en varias categorías como son: seguridad funcional, coordinación, documentación, certificación, acreditación, administración de configuraciones de sistemas y de seguridad informática y manejo de riesgos.

Este documento se elabora con el objetivo de orientar a la Corporación para dar cumplimiento con lo solicitado en el Decreto 612 de 2018 y todas las consideraciones expuestas, dentro de las cuáles se encuentra el decreto 1078 de 2015 y los instrumentos para implementar la Estrategia de Gobierno Digital dentro de los cuales se exige la elaboración por parte de cada entidad, de un Plan de Seguridad y Privacidad de la Información.

En el presente documento se adoptó la concepción, metodología, lineamientos e instrumentos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC-, que conforman la Estrategia de Gobierno Digital, la cual está soportada en los LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN (PESI) Y El MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

1. OBJETIVO

Liderar y establecer las estrategias para la gestión de seguridad y privacidad de la Información en La Empresa de Aseo de Bucaramanga que permitan minimizar los riesgos de pérdida de activos de la información y estén alineadas a la estrategia y modelo integrado de gestión y acordes con las necesidades de la Entidad y los lineamientos del programa de Gobierno Digital.

1.1. Objetivos específicos

El PESI de La Empresa de Aseo de Bucaramanga cuenta con los siguientes objetivos específicos acordes con las necesidades de la Entidad y las dimensiones deGobierno Digital:

- Definir las responsabilidades relacionadas con el manejo de la seguridad, durante el transcurso del año.
- Establecer una metodología de gestión de la seguridad clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Garantizar que los usuarios tienen acceso a la información a través medidas de seguridad con la garantía de calidad y confidencialidad.
- Garantizar la continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.
- Definir el plan para la transición de IPv4 a IPv6 .
- Integración con otros sistemas de gestión.

2. ALCANCE DEL PESI

El PESI (Plan Estratégico de las Seguridad de la Información y Comunicaciones) tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de los procesos que se ejecutan en La Empresa de Aseo de Bucaramanga y será actualizado anualmente; estos apoyarán el cumplimiento de los procesos y objetivos propuestos por las diferentes dependencias de la Entidad y está articulado de manera global en relación con la seguridad de la información.

3. MARCO NORMATIVO

Ley 527 de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo

introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información. (CONGRESO NACIONAL, 1999).

CONPES 3670 de 2010. "Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones".

CONPES 3701 de 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Ley 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 594 de 2000. "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. (CONGRESO DE LA, 2014)

Decreto 103 de 2015: Por la cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información. (PRESIDENCIA DE LA, 2015)

Decreto 2609 de 2012: Por el cual se dictan disposiciones en materia de gestión documental y gestión documental electrónica. (MINISTERIO DE, 2012)

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS, 2012)

Ley 1273 de 2009: Ley la cual se crea y se protege el bien jurídico de la información y los datos personales.

Ley 1581 de 2012: Ley Estatutaria por la cual se reglamenta el artículo 15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales. (CONGRESO D. C., http://www.alcaldiabogota.gov.co, 2012).

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. (CONGRESO D. L., 2000)

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Empresa de Aseo de Bucaramanga entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementaciónde un Sistema de Gestión de Seguridad de la Información –SGSI- buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de nuestra Corporación y las políticas de Calidad y del SGSST.

Para la Empresa de Aseo de Bucaramanga, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

El contenido de esta política aplica a la entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios, entes de control y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios de La Empresa de Aseo de Bucaramanga.

- Garantizar la continuidad de la corporación frente a incidentes.

La Empresa de Aseo de Bucaramanga ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de La Empresa de Aseo de Bucaramanga:

- La Empresa de Aseo de Bucaramanga ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- LA EMPRESA DE ASEO DE BUCARAMANGA protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

- LA EMPRESA DE ASEO DE BUCARAMANGA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- LA EMPRESA DE ASEO DE BUCARAMANGA protegerá su información de las amenazas originadas por parte del personal.

- LA EMPRESA DE ASEO DE BUCARAMANGA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- LA EMPRESA DE ASEO DE BUCARAMANGA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- LA EMPRESA DE ASEO DE BUCARAMANGA implementará control de acceso a la información, sistemas y recursos de red.

- LA EMPRESA DE ASEO DE BUCARAMANGA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- LA EMPRESA DE ASEO DE BUCARAMANGA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- LA EMPRESA DE ASEO DE BUCARAMANGA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- LA EMPRESA DE ASEO DE BUCARAMANGA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

5. ANÁLISIS DE LA SITUACIÓN ACTUAL

5.1. Análisis de brecha MSIP

Apoyados en la herramienta "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD" se obtuvieron los siguientes resultados de análisis de brecha sobre la efectividad de los controles:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	100	INEXISTENTE
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	0	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	INEXISTENTE
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	0	100	INEXISTENTE
PROMEDIO EVALUACIÓN DE CONTROLES		**0**	**100**	INEXISTENTE

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD. MinTIC

Con los resultados del análisis de brecha se obtienen que se deben documentar y formalizar las diferentes Directrices, procedimientos, guías, lineamientos y acuerdos de confidencialidad con miras a garantizar la confiabilidad de la información de la entidad.

Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

Se debe formalizar el procedimiento de levantamiento de activos de información con sus políticas y procedimientos de evaluación previamente definidos.

En cuanto a la madurez del MSPI se tiene el siguiente análisis.

ID REQUISITO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
LIMITE DE MADUREZ INICIAL	360	260	MENOR	440	MENOR	600	MENOR	780	MENOR	980	MENOR
LIMITE DE MADUREZ GESTIONADO	**415**	0		460	MENOR	660	MENOR	880	MENOR	1100	MENOR
LIMITE DE MADUREZ DEFINIDO	360	0		0		660	MENOR	880	MENOR	1100	MENOR
LIMITE DE MADUREZ GESTIONADO CUANTITATIVAMENTE	304	0		0		0		660	MENOR	880	MENOR
LIMITE DE MADUREZ OPTIMIZADO	528									1660	MENOR

5.2. Análisis de brecha Transición de IPv4 a IPv6.

Se proyecta para el 2022 llevar a cabo la adopción del protocolo de IPV6 en Dual- Stack para aumentar la capacidad de direcciones IP disponibles: IPV6 utiliza direcciones IP de 128 bits, lo que proporciona un espacio de direcciones mucho más grande en comparación con IPV4. Esto significa que las empresas pueden asignar direcciones IP únicas a un número mucho mayor de dispositivos conectados a la red, lo que es especialmente importante a medida que se agregan más dispositivos IoT y otros sistemas a la infraestructura de la empresa.

Mejorar la seguridad de la red: IPV6 incluye características de seguridad integradas, como la autenticación y el grabado, lo que ayuda a proteger la red y los datos de la empresa contra amenazas de seguridad en línea.

Mejorar el rendimiento de la red: IPV6 incluye mejoras en el rendimiento de la red, como un enrutamiento más eficiente y una menor sobrecarga de la red debido a la necesidad de NAT (traducción de direcciones de red).

Acceder a servicios y aplicaciones basadas en IPV6: A medida que más empresas y servicios migran a IPV6, las empresas que no adoptan este protocolo pueden enfrentar problemas de compatibilidad y conectividad. Al adoptar IPV6, las empresas pueden garantizar que sus sistemas y servicios puedan conectarse y utilizar aplicaciones y servicios basados en IPV6.

En resumen, la adopción del protocolo IPV6 en una empresa permite una mayor capacidad de direcciones IP, una mejor seguridad y rendimiento de la red, y acceso a servicios y aplicaciones basadas en IPV6.

5.3. Gestión de Información

ACCESO A LA INFORMACIÓN

Consulta en Línea trámites e PQRDS– PÁGINA WEB – Boletines y Comunicados – Reportes – Estadísticas – Datos

Abiertos - Desarrollo de Plan de implementación
Bodegas de Datos Agrupado – RNBD
Servidores dedicados 192.168.1.6 Server- EMAB y plan de contingencia 192.168.1.8 para replicación de sitio.

SISTEMAS DE INFORMACIÓN

- Arco_sis Plus – ERP Corporativo

6 ANÁLISIS DE RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN

Acordes con la información contenida en la "Guía No. 7: Guía de gestión de riesgos"[5] y la "Guía para la Administración del Riesgo" del DAFP[6] se realizó el análisis de riesgo para la seguridad de la información en la Corporación.

Se deben identificar los diferentes factores de riesgo, catalogarlos para llegar a establecer los debidos controles con el objetivo de llegar a obtener riesgos de bajo control, establecer sus debidas acciones asociadas a un indicador para poder llevar a cabo su respectivo seguimiento.

7 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se relacionan los procedimientos que se encuentran en el Sistema de Gestión relacionado con los procedimientos requeridos en la "Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información."

7.1 Seguridad Del Recurso Humano:
Se encuentra definido en los procedimientos de Secretaria General, para la contratación de personal de la entidad

7.2 Gestión De Activos:
Se encuentra definido en los procedimientos para adquisición de activos, Gestión informática y Manual Implementación TICs.

7.3 Control De Acceso:
Se encuentra definido en el procedimiento Gestión informática y el Manual Implementación TICs."

7.4 Criptografía: N/A
Ya que la información que se maneja en la entidad no se requiere la encriptación de esta.

7.5 Seguridad Física Y Del Entorno:
Se encuentra definido en El manual Implementación TICs.

7.6 Seguridad De Las Operaciones:
Se encuentra definido en El manual Implementación TICs.

7.7 Seguridad De Las Comunicaciones:
Se encuentra definido en El manual Implementación TICs.

7.8 Relaciones Con Los Proveedores:
Se encuentra definido en los procedimientos jurídicos y el Manual de Contratación.

7.9. Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información:
Se encuentra definido en el PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI, Procedimiento de Gestión informática y en El manual Implementación TICs.

7.10. Gestión De Incidentes De Seguridad De La Información:
Se encuentra en el Documento de políticas y protocolo, 4.11. Protocolo de Gestión de Incidentes de Seguridad.

7.11. Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio:
Se encuentra definido en el Documento PL-TICS-002 Plan de contingencia.

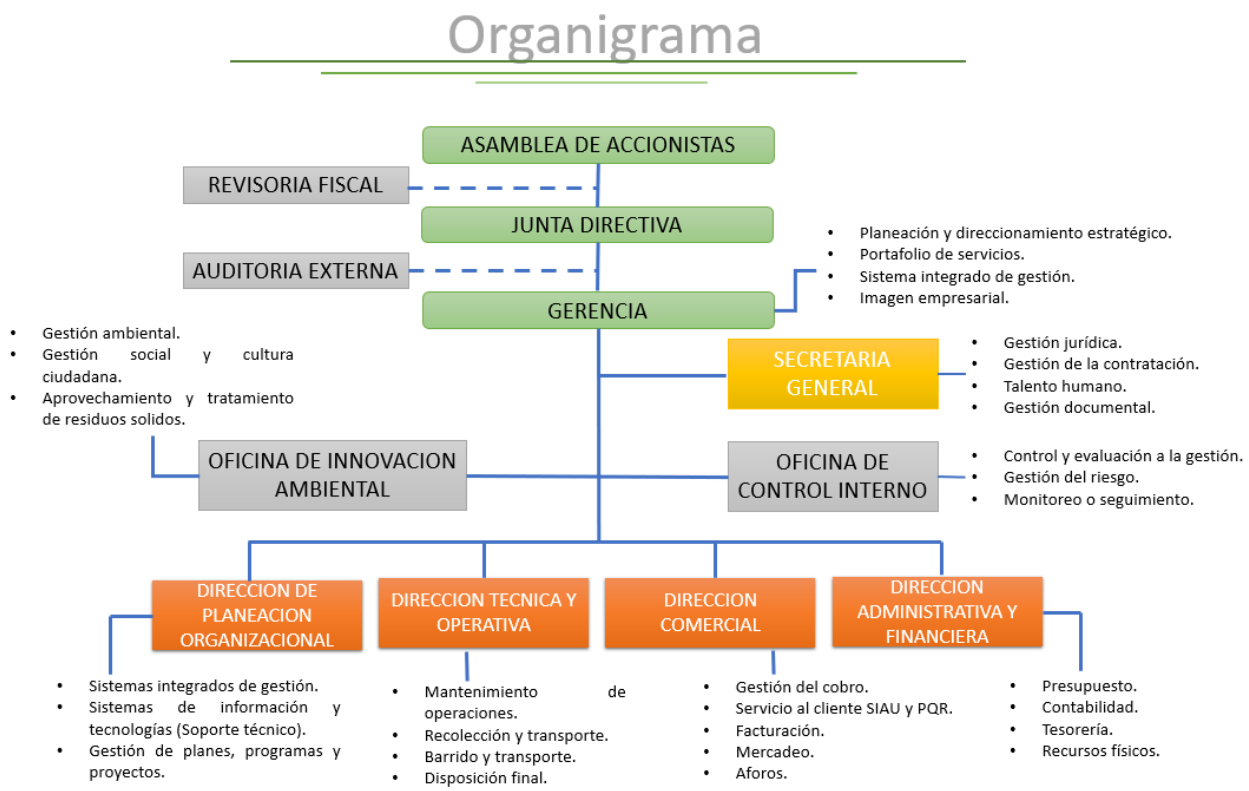
7.12. Plan de sensibilización y apropiación del MSPI para toda la entidad.
Se programarán las actividades relacionadas con la seguridad de la información cada semestre o cuando surjan cambios relevantes y se haga necesario hacerlas de inmediato.

8 ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

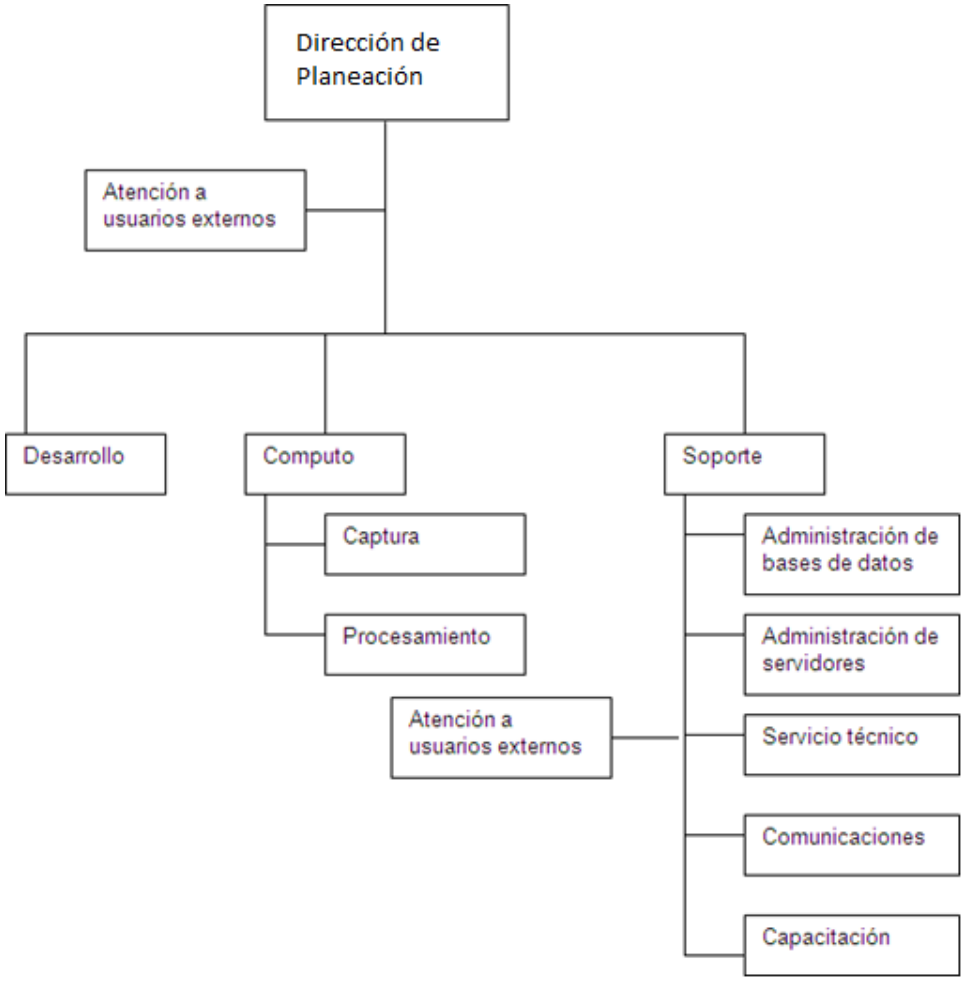
8.1 Gobierno de SI

Basados en la "Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información" desarrollado por MINTIC y el organigrama de la Corporación se define el siguiente de SI.

Organigrama Corporativo



Organigrama de SI



8.2 Responsable de Seguridad de la Información:

En La Empresa de Aseo de Bucaramanga se define como responsable de Seguridad de la Información al Profesional de TICs y de Soporte conforme a las funciones de los cargos en cabeza de la Dirección de Planeación Organizacional.

Por recomendación de la "Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información" se deben desarrollar proyectos de TI y SI, para lo cual la dirección del proyecto está en manos del responsable de SI.

8.3 Equipo del Proyecto:

En la corporación se ha tercerizado la prestación de los servicios de TI, tales como soporte técnico, página web, Aplicativos como Arco_Sis Plus, etc. Cada contrato tiene definido un coordinador y un supervisor, los cuales conforman el equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de

cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

9 SEGUIMIENTO Y REVISIÓN DEL MSPI

- Procedimientos de actualización, seguimiento, revisión y otros controles MSPI

  Se proyecta formalizar el procedimiento para actualización, seguimiento revisión y demás controles al inicio del año 2022.

- Los registros exigidos por la norma ISO 27001 y el MSPI, ej. Un libro de visitantes, informes de auditoría y formatos de autorización de acceso diligenciados.

10 PLANIFICACIÓN DE ACTIVIDADES DEL MSPI

De acuerdo con los objetivos del MSPI se tienen las siguientes actividades:

Componente	Actividades	Año1	Año2	Año3	Año4
1. FASE DE PLANIFICACIÓN	1.1 Revisión de Políticas de Seguridad y Privacidad de la Información	Actualizar, documentar, aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas	Actualizar, aprobar y divulgar Políticas
	1.2. Revisión Procedimientos de Seguridad de la Información.	Actualizar Procedimientos	Actualizar Procedimientos	Actualizar Procedimientos	Actualizar Procedimientos
	1.3. Roles y Responsabilidades de Seguridad	Definir y aprobar Roles y responsabilidades	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades
	1.4. Identificación, documentación y aprobación de activos de Información.	Identificar activos de información y documentar.	Documentar y aprobar activos de información	Actualizar activos de información	Actualizar activos de información
	1.5. Identificación, Valoración YTratamiento de Riesgos.	Actualizar y documentar Riesgos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos
	1.6. Capacitación y sensibilización	Diseñar y aprobar programas yplanes para los funcionarios sobre conciencia y comunicación de las políticas	Funcionarios toman conciencia de la seguridad y privacidad de la información.	Ejecutar planes de toma de Conciencia, comunicación y divulgación.	Ejecutar planes de toma de Conciencia, comunicación y divulgación.
	1.7. Implementar el Modelo de Seguridad y Privacidad de la Información	Alcanzar Madurez Inicial	Alcanzar Madurez Gestionado	Alcanzar Madurez Definido	Alcanzar Madurez gestionado cuantitativamente

Componente	Actividades	Año1	Año2	Año3	Año4
2. FASE DE IMPLEMENTACIÓN	2.1. Planificación y Control Operacional	Definir documentación para el control operacional	Aprobar la documentación	Ajustar de la documentación	Ajustar de la documentación
	2.2. Implementación del plan de tratamiento de riesgos	Verificar inicialmente ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos
	2.3. Indicadores De Gestión	Elaborar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión
	2.4. Plan de Transición de IPv4 a IPv6	Elaborar plan de transición	Implementar plan de transición	Implementar y realizar seguimiento plan de transición	Implementar y realizar seguimiento plan de transición
3. FASE DE EVALUACIÓN DE DESEMPEÑO	3.1. Plan de revisión y seguimiento a la implementación del MSPI	Revisar el MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI
	3.2. Plan de Ejecución de Auditorias	Planear y ejecutar auditorías	Planear y ejecutar auditorías	Planear y ejecutar auditorías	Planear y ejecutar auditorías
4. FASE DE MEJORA CONTINUA	4.1. Plan de mejora continua	Documentar el plan de mejoramiento.	Documentar el plan de Mejoramiento.	Documentar el plan de Mejoramiento.	Documentar el plan de mejoramiento.
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI	Documentar el seguimiento al plan de Mejoramiento.	Documentar el seguimiento al plan de Mejoramiento.	Documentar el seguimiento al plan de Mejoramiento.	Documentar el seguimiento al plan de mejoramiento.
	4.3 Resultados del plan de ejecución de	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan

Componente	Actividades	Año 1	Año 2	Año 3	Año 4
	Auditorías y revisiones independientes al MSPI.				
5. MODELO DE MADUREZ	5.1. Autodiagnóstico nivel de madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.2. Identificación del nivel madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.3. Análisis de brecha	Realizar Análisis	Realizar Análisis	Realizar Análisis	Realizar Análisis
6. PRIVACIDAD DE LA INFORMACIÓN	6.1. Contar con una herramienta de análisis sobre impacto en la privacidad	Realizar la Herramienta de análisis sobre impacto en la privacidad	Realizar la herramienta de análisis sobre impacto en la privacidad	Ajustar la herramienta	Ajustar la herramienta
	6.2. Descripción de los flujos de información	Documentar procesos	Revisar procesos documentados	Revisar procesos documentados	Revisar procesos documentados
	6.3. Identificar los riesgos de privacidad	Elaborar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad
7. ADOPCIÓN DEL PROTOCOLO IPv6	7.1. Plan y estrategia de transición de IPv4 a IPv6.	Verificar y actualizar el plan	Verificar y actualizar el plan	Verificar y actualizar el plan	Verificar y actualizar el plan
	7.2. Implementación del plan y estrategia de transición de IPv4 a IPv6.	Implementar el plan	Implementar el plan	Implementar el plan	Implementar el plan
	7.3. Plan de pruebas de funcionalidad de IPv4 a IPv6.	Realizar pruebas	Realizar pruebas	Realizar pruebas	Realizar pruebas

Con base en estas actividades se elaborarán los indicadores y un tablero de control para el seguimiento de estos indicadores.

10.1 Proyección de presupuesto de área de SI Presupuesto por líneas de acción:

Componente	Actividades	Recurso Humano	Recurso económico o tecnológico
1. FASE DE PLANIFICACIÓN	1.1 Revisión de Políticas de Seguridad y Privacidad de la Información	X	
	1.2. Revisión Procedimientos de Seguridad de la Información.	X	
	1.3. Roles y Responsabilidades de Seguridad	X	X
	1.4. Identificación, documentación y aprobación de activos de información.	X	
	1.5. Identificación, Valoración Y Tratamiento de Riesgos.	X	
	1.6. Capacitación y sensibilización	X	X
	1.7. Implementar el Modelo de Seguridad y Privacidad de la Información	X	X
2. FASE DE IMPLEMENTACIÓN	2.1. Planificación y Control Operacional	X	X
	2.2. Implementación del plan de tratamiento de riesgos	X	X
	2.3. Indicadores De Gestión	X	
	2.4. Plan de Transición de IPv4 a IPv6	X	X
3. FASE DE EVALUACIÓN DE DESEMPEÑO	3.1. Plan de revisión y seguimiento a la implementación del MSPI	X	X
	3.2. Plan de Ejecución de Auditorias	X	
4. FASE DE MEJORA CONTINUA	4.1. Plan de mejora continua	X	X
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI	X	
	4.3 Resultados de ejecución de auditoría y revisiones independientes al MSPI.	X	
5. MODELO DE MADUREZ	5.1. Autodiagnóstico nivel de madurez	X	
	5.2. Identificación del nivel madurez	X	
	5.3. Análisis de brecha	X	
6. PRIVACIDAD DE LA INFORMACIÓN	6.1. Contar con una herramienta de análisis sobre impacto en la privacidad	X	X
	6.2. Descripción de los flujos de información	X	
	6.3. Identificar los riesgos de privacidad	X	
7. ADOPCIÓN DEL PROTOCOLO IPv6	7.1. Plan y estrategia de transición de IPv4 a IPv6.	X	X
	7.2. Implementación del plan y estrategia de transición de IPv4 a IPv6.	X	X
	7.3. Plan de pruebas de funcionalidad de IPv4 a IPv6.	X	X

11. Plan de Comunicaciones del PESI

Para alcanzar el logro de los objetivos de este plan, las actividades se encaminan a lograr una nivelación de funcionarios y usuarios por medio de tres ejes fundamentales:

- Formación.
- Acceso a la tecnología.
- Procesos institucionales acordes.

Para lograr este punto, se consideraron las siguientes acciones:

Incluir en el plan de capacitación programas de capacitación, entrenamiento y sensibilización a la incorporación de Sistemas de Información, en temas relacionados con:

- Administración De Contraseñas
- Uso Y Manejo De Inventario
- Malware y sus diferentes tipos
- Software Permitido/Prohibido En La Entidad
- Políticas Organizacionales Relacionadas Con Seguridad De La Información
- Uso De Dispositivos De La Entidad Fuera De Las Instalaciones
- Uso De Correo Electrónico E Identificación De CorreosSospechosos
- Seguridad En El Puesto De Trabajo
- Uso Apropiado De Internet
- Temas de control de acceso a los sistemas (privilegios, separación de roles)
- Política De Escritorio Limpio
- Ingeniería Social
- Gestión De Incidentes (Como reportar, que puedo reportar)
- Spam
- "Shoulder Surfing" Backups Y Recuperación
- Cambios En Los Sistemas
- Amenazas Y Vulnerabilidades Comunes
- Roles Y Responsabilidades En La Entidad

11.1. Alcance

El alcance del plan actual va ligado con todas aquellas personas que se encuentran relacionadas de manera directa e indirecta con el soporte que debe darse a funcionarios, decisores y usuarios en materia de SI de La Empresa de Aseo de Bucaramanga.

12. Historial de cambios

VERSIÓN	DESCRIPCIÓN	FECHA
1.0	Creación de documento	01 de febrero de 2023