# **OBJETIVO**

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2024-2027.

1. **ALCANCE**

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la Empresa de Aseo de Bucaramanga S.A. E.S.P de 2024 - 2027.

Igualmente, en la medida en que avancen los proyectos ejecutados y en respuesta a las dinámicas del entorno y del servicio, se llevará a cabo una programación e iteración del Plan Estratégico de Tecnologías de la Información (PETI). Estas acciones se realizarán en el marco de metodologías que se ajusten a las necesidades cambiantes previamente identificadas.

# La presente política se debe cumplir por todos los trabajadores, terceros y practicantes que se encuentran involucrados en los diferentes procesos de la Empresa de Aseo de Bucaramanga S.A.E.S.P. y, adicionalmente, por los ciudadanos, persona naturales o jurídicas, nacionales o extranjera que sin tener relación laboral o contractual con la EMAB S.A. E.S.P. tengan acceso a sus instalaciones y/o servicios tecnológicos.

1. **RESPONSABLE**

El responsable de liderar el Plan Estratégico de Seguridad de la información es el profesional de Tics con la colaboración de todos los directivos y funcionarios de la Empresa de Aseo de Bucaramanga S.A. E.S.P.

En el desarrollo de las actividades para definir y gestionar la estrategia de TI participan los siguientes roles:

| **Rol** | **Responsabilidades definidas** |
| --- | --- |
| Director(a) Planeación Organizacional | Liderar la definición y ejecución de la estrategia de TI. |
| Equipo de Tecnologías y Sistemas de Información | Concebir la estrategia de TI y planear la manera en que se puede llevar a cabo, orientando los esfuerzos desde sus especialidades hacia objetivos comunes |
| Líderes funcionales de proyectos que incorporen Componentes TI | Coordinar y orientar desde el punto de vista funcional proyectos de TI o que incorporen componentes de TI. |
| Oficial de Seguridad de la Información | Liderar la definición e implementación de la política de seguridad de la información y la implementación del modelo de seguridad y privacidad en la entidad. |
| Equipo de Oficinas asesoras de planeación | Participar y apoyar en la definición de fuentes de recursos para identificar posibilidades de financiamiento Apoyar la ejecución de auditorías de cumplimiento para verificar la adopción de los componentes de TI. |
| Equipos de comunicación | Participar en la definición de las estrategias de comunicación, divulgación y promoción de los componentes de TI y de los cambios apoyados con tecnología definiendo los mensajes clave, canales y formatos más adecuados de acuerdo con las necesidades identificadas. Diseñar los recursos requeridos para divulgar los mensajes clave de las estrategias de comunicación definidas Participar en la ejecución de las estrategias de comunicaciones. |
| Equipo de Talento Humano | Participar en la definición del plan de formación y plan de capacitación y entrenamiento e integrar y alinear con los planes de la entidad. Apoyar la ejecución del plan de formación y el plan de capacitación y entrenamiento. |
| Directivos de la entidad | Orientar y plantear las necesidades y los objetivos estratégicos y de la gestión requerida que puedan ser habilitadas con tecnologías de información Patrocinar e impulsar el uso de las TIC en la entidad. |

1. **CONDICIONES GENERALES**

La seguridad y privacidad de la información, como un componente integral de la Estrategia de Gobierno Digital, permite alinear la estrategia con los siguientes componentes:

* + - TIC para la Gestión:

Contribuye al uso estratégico de las tecnologías de la información al formular e implementar un modelo de seguridad enfocado en preservar la confidencialidad, integridad y disponibilidad de la información.

Su aplicación se traduce en el cumplimiento de la misión y los objetivos estratégicos de la entidad.

* + - TIC para Servicios:

Apoya el tratamiento de la información utilizada en trámites y servicios, observando en todo momento las normas de protección de datos personales y otros derechos garantizados por la ley.

Asegura que el acceso público a determinada información esté sujeto a las regulaciones pertinentes.

* + - TIC para Gobierno Abierto:

Facilita la construcción de un estado más transparente, colaborativo y participativo al garantizar controles de seguridad y privacidad en la información proporcionada.

Asegura que las interacciones de información con ciudadanos, otras entidades y la empresa privada sean confiables.

# **MARCO NORMATIVO**

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,](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)

# **DESCRIPCIÓN**

# **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 implementación de 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, 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

# **ANÁLISIS DE LA SITUACIÓN ACTUAL**

1. 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 | 60 | 100 | **EFECTIVO** |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 39 | 100 | **REPETIBLE** |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 20 | 100 | **INICIAL** |
| A.8 | GESTIÓN DE ACTIVOS | 33 | 100 | **REPETIBLE** |
| A.9 | CONTROL DE ACCESO | 33 | 100 | **REPETIBLE** |
| A.10 | CRIPTOGRAFÍA | 0 | 100 | **INEXISTENTE** |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 35 | 100 | **REPETIBLE** |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 16 | 100 | **INICIAL** |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 21 | 100 | **REPETIBLE** |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 30 | 100 | **REPETIBLE** |
| A.15 | RELACIONES CON LOS PROVEEDORES | 20 | 100 | **INICIAL** |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 31 | 100 | **REPETIBLE** |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 60 | 100 | **EFECTIVO** |
| A.18 | CUMPLIMIENTO | 34 | 100 | **REPETIBLE** |
| ***PROMEDIO EVALUACIÓN DE CONTROLES*** | **31** | **100** | **REPETIBLE** |

**INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD. MinTIC**

Con los resultados del análisis de brecha se obtienen que se deben implementar una serie de controles en los dominios de criptografía, seguridad de las operaciones, relación con los proveedores de tecnología y seguridad de los recursos humanos en miras a garantizar la confiabilidad de la información de la entidad.

1. Se debe contar con un inventario de activos de información, revisado y aprobado por la alta dirección.
2. 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.
3. 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:

|  |  |  |
| --- | --- | --- |
| mastic - Intelligent Training | INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICAHOJA LEVANTAMIENTO DE INFORMACIÓN |  |
|  |
|  |
|  |
| **EMPRESA DE ASEO DE BUCARAMANGA SA ESP** |  |
|  |
|  |
|  |
|  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| **ID REQUISITO** | **CALIFICACIÓN OBTENIDA** | **NIVEL 1INICIAL** | **CUMPLIMIENTONIVEL INICIAL** | **NIVEL 2GESTIONADO** | **CUMPLIMIENTONIVEL GESTIONADO** | **NIVEL 3DEFINIDO** | **CUMPLIMIENTONIVEL DEFINIDO** | **NIVEL 4GESTIONADOCUANTITATIVAMENTE** | **CUMPLIMIENTONIVEL 4GESTIONADOCUANTITATIVAMENTE** | **NIVEL 5OPTIMIZADO** | **CUMPLIMIENTONIVEL 5OPTIMIZADO** |  |
| LIMITE DE MADUREZ INICIAL | 420 | 260 | MENOR | 440 | MENOR | 600 | MENOR | 780 | MENOR | 980 | MENOR |  |
| LIMITE DE MADUREZ GESTIONADO | **388** | 0 |   | 460 | MENOR | 660 | MENOR | 880 | MENOR | 1100 | MENOR |  |
| LIMITE DE MADUREZ DEFINIDO | 265 | 0 |   | 0 |   | 660 | MENOR | 880 | MENOR | 1100 | MENOR |  |
| LIMITE DE MADUREZ GESTIONADO CUANTITATIVAMENTE | 206 | 0 |   | 0 |   | 0 |   | 660 | MENOR | 880 | MENOR |  |
| LIMITE DE MADUREZ OPTIMIZADO | 372 |   |   |   |   |   |   |   |   | 1660 | MENOR |  |

Con base en los resultados obtenidos del autodiagnóstico y el nivel de madurez actual de la entidad, se identifican los aspectos más pertinentes en cada uno de los dominios del sistema que requieren mejoras. El objetivo es llevar a la entidad a alcanzar un nivel mínimo aceptable en el sistema:

|  |  |  |  |
| --- | --- | --- | --- |
| **DOMINIO** | **SITUACION ACTUAL** | **SITUACION DESEADA** | **EJECUCION** |
| CONTROL DE ACCESO | No se cuenta con procedimientos de segregación de roles. No se cuenta con documento de clasificación de la información que permita dar manejo a la información  | Lineamientos establecidos para el control de segregación, con el fin de mitigar los riesgos asociados al conflicto de interés o responsabilidades  | Primer Trimestre  |
| ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | En los aspectos de seguridad del teletrabajo y uso de dispositivos móviles   internos y externos, no se cuenta con un lineamiento general o manual de políticas, ocasionando gran exposición de la infraestructura tecnológica de la Entidad. | Inclusión de política general para control de Teletrabajo. | Tercer Trimestre |
| SEGURIDAD DE LOS RECURSOS HUMANOS | No se cuentan documentos por parte del área de talento humano con los controles de selección, ejecución y desvinculación de usuarios. | Establecimiento de lineamientos en un documento de manera formal por parte del área de talento humano del Sistema de Gestión de Seguridad de la información | Segundo Trimestre  |
| CRIPTOGRAFÍA | No se cuenta con procedimientos sobre la gestión de los controles criptográficos. | Establecer procedimientos sobre controles criptográficos | Tercer Trimestre |
| SEGURIDAD DE LAS OPERACIONES | No se evidencia procedimiento para monitoreo gestión de logs o herramientas de la plataforma tecnológica de tal forma que se pueda realizar una detección temprana de eventos de seguridad, que mitiguen la posibilidad de materialización de riegos que puedan ocasionar incidentes de seguridad de la información. | Procedimientos establecidos y liberados para monitoreo y gestión de logs de la infraestructura tecnológica periódica por parte de los responsables de las plataformas. | Tercer Trimestre |
| ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | No se cuenta con procedimientos para Adquisición, desarrollo y mantenimiento de software. Donde se involucren los requisitos mínimos de seguridad para los sistemas de información. | Procedimientos para adquisición, mantenimiento y desarrollo de software. Con definición de metodología unificada para todos los desarrollos y con estándares de desarrollo seguro de software, liberados y apropiados. | Segundo Trimestre  |

* 1. **Gestión de Información**

**ACCESO A LA INFORMACIÓN**

Se cuenta con infraestructura propia: el servidor principal con IP 192.168.1.6 Server- EMAB, el servidor para el aplicativo de podas <http://200.116.213.34/> y el servidor para plan de contingencia con IP 192.168.1.8 para replicación.

* Para el manejo de información se cuenta con el ERP ARCO\_SIS PLUS con la información comercial, financiera, de contratación, talento humano
* Se cuenta con acceso al portal de pqr <https://pqr.emab.gov.co/> para la radicación, consulta y seguimiento en Línea trámites e PQRDS– PÁGINA WEB – Datos Abiertos – Se tiene actualmente registro en el portal de Datos abiertos y bases de datos registradas, se debe retomar y actualizar para desarrollar Plan de implementación de acuerdo a actualización de lineamientos de MinTIC.
* Bodegas de Datos Agrupado – Levantamiento de bases de datos para reporte y registro en el RNBD.

**SISTEMAS DE INFORMACIÓN**

* El principal sistema que se tiene es el ERP Arco\_sis Plus, en donde se maneja la información Financiera, Comercial, Tarifaria, Nominal, correspondencia y de Contratación.
* Se maneja ArcGIS para el manejo de georreferenciación en la parte Operativa con la prestación del servicio.

# **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 DAFP6 se realizó el análisis de riesgo para la seguridad de la información en donde se identifican los riesgos a tratar para la vigencia 2024.

Se identifican los diferentes factores de riesgo y se catalogan para llegar a establecer los debidos controles con el objetivo de llegar a obtener riesgos de bajo control, se establecen sus debidas acciones para su respectivo seguimiento, los diferentes riesgos identificados se plasmarán en la matriz de riesgos informáticos con su debido tratamiento Mapa de riesgos TICS 2024.xls.

# **INSTRUCCIONES 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.”

* Seguridad Del Recurso Humano: Se encuentra definido en los procedimientos de secretaria general, para la contratación de personal de la entidad
* Gestión De Activos: Desde el área de sistemas para manejo de equipos informáticos se encuentra definido en los procedimientos para adquisición de activos, Gestión informática y Manual Implementación TICs.
* Control De Acceso: Se encuentra definido en el procedimiento Gestión informática y el Manual Implementación (TICs. M-TICS-001 MANUAL IMPLEMENTACION TICS V.1.docx)

* Criptografía: N/A, Por la información que actualmente se maneja en la entidad no se requiere la encriptación de esta.

* Seguridad Física Y Del Entorno: Se encuentra definido en El manual Implementación TICs. (M-TICS-001 MANUAL IMPLEMENTACION TICS V.1.docx)
* Seguridad De Las Operaciones: Se encuentra definido en El manual Implementación TICs. (M-TICS-001 MANUAL IMPLEMENTACION TICS V.1.docx)
* Seguridad De Las Comunicaciones: Se encuentra definido en El manual Implementación (TICs. M-TICS-001 MANUAL IMPLEMENTACION TICS V.1.docx )
* Relaciones Con Los Proveedores: Se encuentra definido en los procedimientos jurídicos y el Manual de Contratación.
1.
* 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. (PL-TICS-001 Plan estratégico de Tecnología PETI V.4.docx, PR-TICS-004 PROCEDIMIENTO GESTIÓN INFORMÁTICA V.1.docx, M-TICS-001 MANUAL IMPLEMENTACION TICS V.1.docx)
1.
* 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. (Documento de Políticas y Protocolos.docx)
* 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 V.1.docx).

# **ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

* 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 EMAB S.A. E.S.P.



Organigrama de SI



* 1. **Equipo del Proyecto:**

Algunos de los servicios ofrecidos desde TI como el alojamiento de la página web, soporte Aplicativos como Arco\_Sis Plus, tienen contrato con su debido supervisor asignado, 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.

# **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 para el año 2024.

# Seguimiento de 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.

# **PLANIFICACIÓN DE ACTIVIDADES DEL MSPI**

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Componente** | **Actividades** | **Año1**  | **Año2** | **Año3** | **Año4** | **Fecha de ejecución** |
|   **1. FASE DE PLANIFICACIÓN**  | 1.1 Revisión de Política de Seguridad y Privacidad de la Información | Revisar y actualizar si se requiere, aprobar y divulgar Política  | Revisar y actualizar si se requiere, aprobar y divulgar Política  | Revisar y actualizar si se requiere, aprobar y divulgar Política  | Revisar y actualizar si se requiere, aprobar y divulgar Política  |  Segundo Trimestre de cada año |
| 1.1.1 Revisar y actualizar procedimiento para tratamiento a Bases de Datos | Actualizar, documentar, aprobar y divulgar Políticas o lineamientos pendientes por desarrollar | Actualizar, documentar, aprobar y divulgar Políticas o lineamientos pendientes por desarrollar | Actualizar, documentar, aprobar y divulgar Políticas o lineamientos pendientes por desarrollar | Actualizar, documentar, aprobar y divulgar Políticas o lineamientos pendientes por desarrollar |  Primer Trimestre de cada año |
| 1.1.2 Levantamiento de Bases de Datos | Actualizar, documentar, y reportar RNBD | Actualizar, documentar, y reportar RNBD | Actualizar, documentar, y reportar RNBD | Actualizar, documentar, y reportar RNBD |
| 1.2 Inclusión de política general para control de Teletrabajo. | Elaboración de política general para control de Teletrabajo. | Revisar y actualizar si se requiere, aprobar y divulgar Política  | Revisar y actualizar si se requiere, aprobar y divulgar Política  | Revisar y actualizar si se requiere, aprobar y divulgar Política  | Tercer Trimestre |
| 1.2. Revisión Procedimiento de Seguridad de la Información. | Revisar y actualizar Procedimiento si se requiere | Revisar y actualizar Procedimiento si se requiere | Revisar y actualizar Procedimiento si se requiere | Revisar y actualizar Procedimiento si se requiere | Segundo Trimestre de cada año |
| 1.4. Solicitud de documentación y aprobación de activos de Información. | Identificar activos de información y documentar para tratamiento en caso de que se requiera. | Revisar y actualizar para tratamiento de activos de información en caso de que se requiera. | Revisar y actualizar para tratamiento de activos de información en caso de que se requiera. | Revisar y actualizar para tratamiento de activos de información en caso de que se requiera. |  Primer Trimestre de cada año |
| 1.6. Capacitación sensibilización | Diseñar y aprobar plan para los funcionarios sobre conciencia y comunicación de las políticas | Diseñar y aprobar plan para los funcionarios sobre conciencia y comunicación de las políticas | Diseñar y aprobar plan para los funcionarios sobre conciencia y comunicación de las políticas | Diseñar y aprobar plan para los funcionarios sobre conciencia y comunicación de las políticas |  Primer Trimestre de cada año |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Componente** | **Actividades** | **Año1** | **Año2** | **Año3** | **Año4** |
| **2. FASE DE** **IMPLEMENTACIÓN** | 2.1. Planificación y Control Operacional | Definir documentaciónPara 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 tratamiento de riesgos | Verificar ejecución de acciones para el tratamiento de riesgos | Verificar ejecución de acciones para el tratamiento de riesgos | Verificar ejecución de acciones para el tratamiento de riesgos |
| **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 |
| **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. |
| 4.3 Resultados del planDe ejecución de  | Socializar resultados del plan | Socializarresultados del plan | Socializarresultados del plan | Socializarresultados del plan |
| **Componente** | **Actividades** | **Año 1 Año 2** | **Año 3** | **Año 4** |
| **5. MODELO DE MADUREZ** | 5.1. Autodiagnóstico nivel de madurez | Realizar Autodiagnóstico | Realizar Autodiagnóstico | Realizar Autodiagnóstico | Realizar Autodiagnóstico |
| 5.2 Identificación del nivel de madurez  |  | Realizar Autodiagnóstico | Realizar Autodiagnóstico | Realizar Autodiagnóstico | Realizar Autodiagnóstico |
| 5.3. Análisis de brecha | Realizar Análisis de brecha | Realizar Análisis de brecha | Realizar Análisis de brecha | Realizar Análisis de brecha |
| 6.2. Descripción de losflujos de información | Documentarprocesos | Revisar procesosdocumentados | Revisar procesosdocumentados | Revisar procesosdocumentados |
| 6.3. Identificar riesgos de privacidad  | los | Elaborar matriz deriesgos de privacidad  | Actualizar matriz de riesgos de seguridad | Actualizar matriz de riesgos de privacidad  | Actualizar matriz deriesgos de privacidad |

**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. Localización, 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 – renovación licenciamiento | **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** |  |
| **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** |  |

#

# **PRESUPUESTO APROBADO PARA 2025**

|  |
| --- |
| **TECNOLOGIA Y LICENCIAS E INFORMATICA** |
| **OBJETO** | **VALOR UNITARIO** | **CANT.** | **VALOR ANUAL** | **SALDO** |
| Servicio de Hosting superior | $ 600.000  | 1 |  $ 600.000  |  $ 600.000  |
| Servicio de Hosting | $ 600.000  | 1 |  $ 600.000  |  $ 600.000  |
| Renovación de la licencia del FORTINET | $ 11.000.000  | 1 | $ 11.000.000 | $ 11.000.000 |
| Renovación del pool asignado por LACNIC para protocolo IPV6 | $ 20.000.000  | 1 | $ 20.000.000  |  $ 20.000.000  |
| Licencia y soporte de correos corporativos en Gmail | $ 55.000.000  | 1 |  $ 55.000.000  |  $ 55.000.000  |
| Permiso licencia de almacenamiento del sitio alterno ubicado en el carrasco | $ 5.200.000  | 1 |  $ 5.200.000  |  $ 5.200.000  |
| Antivirus | $ 28.000.000  | 1 |  $ 28.000.000  |  $ 28.000.000  |
| Licencias de usuario ESRI-ArcGIS | $ 30.000.000  | 1 |  $ 30.000.000  |  $ 30.000.000  |
| Copias Azure copias en la nube | $ 500.000  | 12 |  $ 6.000.000  |  $ 6.000.000  |
| Desarrollo en página web -implementar servicios web  | $ 10.000.000  | 1 |  $ 10.000.000  |  $ 10.000.000  |
| Contrato de mantenimiento de las UPS parte operativa y administrativa de la empresa de Aseo de Bucaramanga  | $ 1.000.000  | 12 | $ 12.000.000  |  $ 12.000.000  |
| Servido Icloud | $ 30.000.000  | 1 |  $ 30.000.000  | $ 30.000.000  |
| Backups equipos | $ 2.000.000  | 10 |  $ 20.000.000  | $ 20.000.000  |
| Tratamientos datos personales | $ 3.000.000  | 12 |  $ 36.000.000  |  $ 36.000.000  |
| SOFTWARE DE SEGUIMIENTO PROCESOS JUIDICIALES | $ 250.000  | 12 | $ 3.000.000  | $ 3.000.000  |
| Equipos de cómputo con licencias (10) | $ 70.000.000  | 10  | $ 70.000.000  |  $ 70.000.000  |
| Herramientas de mantenimiento sistemas | $ 98.763.136  | 1  |  $ 98.763.136  |  $ 98.763.136  |
| **TOTAL** | **$ 365.913.136** |  |  **$ 436.163.136** |  **$ 436.163.136** |

# **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:

Llevar a cabo estrategias de capacitación, entrenamiento y sensibilización a la incorporación de Sistemas de Información con el uso de herramientas como el correo corporativo, 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 a la Información
		- Uso de dispositivos de la entidad fuera de las instalaciones
		- Uso de correo electrónico e identificación de correos sospechosos
		- 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

1. **Historial de cambios**

|  |  |  |
| --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** |
| 1.0 | Creación de documento | 01 de febrero de 2023 |
| 2.0 | Actualización de documento | 03 de Abril de 2024 |
| 3.0 | Actualización de documento | 22 de Enero 2025 |