2025

Modelo de Seguridad y Privacidad de la Información MSPI

Oficina de Información y Comunicación

AMB
AREA METROPOLITANA
DE BARRANQUILLA

Área Metropolitana de Barranquilla

Tabla de contenido

Información del Documento 4
1. INTRODUCCCIÓN 5
2. OBJETIVO GENERAL 5
2.1. Objetivos específicos: 5
3. DEFINICIONES 5
4. PROPÓSITOS DEL MSPI DEL AMB 15
5. MARCO JURÍDICO 16
6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI 18
7. DIAGNÓSTICO 18
8. FASE 1. DE PLANIFICACIÓN 22
8.1. Contexto 24
8.1.1. Comprensión de la entidad y su contexto 24
8.1.2. Necesidades y expectativas de los interesados 25
8.1.3. Definición del Alcance del MSPI 25
8.2. Liderazgo 26
8.2.1. Liderazgo y Compromiso 26
8.2.2. Política de Seguridad y Privacidad de la Información 27
8.2.3. Roles y responsabilidades del MSPI 27
8.3. Planeación 29
8.3.1. Identificación de activos de información e infraestructura critica cibernética 29
8.3.2. Valoración de los riesgos de Seguridad de la Información 32
8.3.3. Plan de Tratamiento de los riesgos de Seguridad de la Información 32
8.4. Soporte 33
8.4.1. Recursos 33
8.4.2. Competencia, toma de conciencia y comunicación 33
9. FASE 2. DE OPERACIÓN 34
9.1.1. Control y Planeación operacional 34
9.1.2. Plan de Tratamiento de riesgos 35
9.1.3. Definición de Indicadores de gestión 35
10. FASE 3. DE EVALUACIÓN Y DESEMPEÑO 36
10.1.1. Seguimiento, medición, análisis y evaluación 36
10.1.2. Auditoría interna 36
10.1.3. Revisión por para de la Dirección 37

11. FASE 4. MEJORAMIENTO CONTINUO 37
11.1.1. Mejora continua y Acciones correctivas y No conformidades 37

Información del Documento

Título:	Modelo de Seguridad y Privacidad de la Información (MSPI)
Archivo:	Entregable 1
Versión:	1
Autor:	Oficina de Información y Comunicación. Profesional Universitario 219-03
Estado:	Aprobado

1. INTRODUCCCIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI) como parte del Sistema de Gestión de Seguridad de la Información (SGSI), compromete a la alta Dirección y al resto de la entidad con la importancia de mantener y garantizar la seguridad de la información que gestiona. El SGSI y el MSPI pretenden contribuir a minimizar los riesgos asociados a la información, mostrando la eficiencia administrativa y asegurando el cumplimiento de las directrices impartidas por la Política de Gobierno Digital en alineación con la norma internacional ISO/IEC 27001, que especifica los requisitos para un Sistema de Gestión de la Seguridad de la Información, en este caso aplicando los estándares de referencia para el Área Metropolitana de Barranquilla.

2. OBJETIVO GENERAL

Establecer e Implementar las actividades del Modelo de Seguridad y Privacidad de la Información MSPI alineadas con la NTC/IEC ISO 27001:2013, la estrategia de gobierno digital, la Política de Seguridad Digital y Continuidad del servicio, en cumplimiento de las disposiciones legales vigentes.

2.1. Objetivos específicos:

- **Establecer** los lineamientos para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
- **Gestionar** los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación del AMB.
- **Identificar** y Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
- **Generar** conciencia de la importancia y apropiación de la Seguridad y Privacidad de la Información como eje transversal de la entidad.

3. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas,

soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).

- **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 27001:2022).
- **Amenaza cibernética:** aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27001:2022).
- **Ataque informático:** Conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.
- **Ataque cibernético:** acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. Este concepto se desarrolla de manera más profunda como ciberataque.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).
- **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).
- **BCP (Business Continuity Planning / Plan de Continuidad de Negocios):** Es un plan logístico detallado de cómo una entidad debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de 8 una interrupción no deseada o desastre.
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **CERT: (Computer Emergency Response Team)** Equipo de Respuesta a Emergencias cibernéticas, por su sigla en inglés. Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.
- **Ciberespacio:** Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias. (Decreto 338 de 2022).

- **Ciberdefensa:** capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética. (Conpes 3995 de 2020).
- **Ciberespionaje:** se utiliza principalmente como un medio para recopilar datos sensibles o clasificados, secretos comerciales u otras formas de propiedad intelectual que pueden ser utilizados por el agresor para crear una ventaja competitiva o vendidos para obtener beneficios financieros. En algunos casos, la violación simplemente pretende causar un daño reputacional a la víctima exponiendo información privada o prácticas empresariales cuestionables.» - Crowdstrike.
- **Ciberincidente:** Cualquier acto malicioso o evento sospechoso que comprometa, o intente comprometer la Seguridad del perímetro electrónico, la Seguridad del primero físico o un activo crítico.
- **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Ciberamenaza**: Cualquier circunstancia o evento con el potencial de impactar negativamente en las operaciones de la organización (incluyendo misión, funciones, imagen o reputación), activos de la organización o individuos a través de un sistema de información mediante acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio. También, el potencial de una amenaza-fuente para explotar con éxito una vulnerabilidad particular del sistema de información. NIST SP 1800-15B.
- **Ciberataque**: Un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por parte de una empresa con el propósito de interrumpir, inutilizar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada. NIST SP 1800-10B de NIST SP 800-30 Rev.1
- **Ciberterrorismo:** es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas.
- **CSIRT: (Computer Security Incident & Response Team)** Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.
- **CSIRT Gobierno:** Equipo de Respuesta a Incidentes de Seguridad en sus siglas en inglés (Computer Security Incident & Response Team), integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan medidas tendientes a prevenir y gestionar incidentes de ciberseguridad de las entidades del estado.

- **CSIRT sectorial:** Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones.
- **CSIRT sectorial crítico:** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos.
- **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.
- **Código malicioso:** Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.
- **COLCERT:** Por sus siglas en inglés **Computer Emergency Response Team**, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual se encuentra enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica cibernética del Estado Colombiano frente a emergencias de Ciberseguridad que atenten y comprometan la seguridad y defensa nacional.
- **Contención de un incidente:** Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.
- **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 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, numeral 3).

- **Denegación del servicio:** Conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema servicio informático.
- **Derecho a la Intimidad:** Protege el ámbito privado del individuo y de su familia como el núcleo humano más próximo. Uno y otra están en posición de reclamar una mínima consideración particular y pública a su interioridad, actitud que se traduce en abstención de conocimiento e injerencia en la esfera reservada que les corresponde y que está compuesta por asuntos, problemas, situaciones y circunstancias de su exclusivo interés. Esta no hace parte del dominio público y, por tanto, no debe ser materia de información suministrada a terceros, ni de la intervención o análisis de grupos humanos ajenos, ni de divulgaciones o publicaciones (Sentencia C-640/10).
- **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).
- **Entorno digital:** Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854).
- **Entorno digital abierto:** Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).
- **Evento:** Un evento es cualquier suceso observable en un sistema o red, como un usuario que se conecta a un recurso compartido de archivos, un usuario que envía un archivo electrónico o un firewall que bloquea un intento de conexión, entre otros.
- **Eventos adversos:** son aquellos que tienen consecuencias negativas, como fallos en un sistema, usos no autorizados de privilegios en un sistema, acceso no autorizados y ejecución de malware.
- **Evento de Seguridad de la Información:** Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 27000:2009].
- **Defacement**: Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia.
- **DoS / DDoS (Denial of Service / Distributed Denial of Service):** Se entiende como denegación de servicio, en términos de seguridad digital, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca

sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

- **DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres):** es un documento formal creado por una organización que contiene instrucciones detalladas con la definición de los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.
- **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 27001:2022).
- **Gobernanza de la seguridad digital para Colombia:** Corresponde al conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.
- **Incidente:** Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y/o prácticas de seguridad básicas.
- **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022).
- **Infraestructura Cibernética (Ic):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO).
- **Infraestructura Crítica Cibernética (ICC):** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. (Decreto 338 de 2022).
- **Infraestructura Estratégica (IE):** Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales.
- **Infraestructura Estratégica Cibernética (IEC):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operación (TO), sobre las que se soporta el funcionamiento de los servicios esenciales.
- **Incidente de seguridad informática:** Una violación o inminente amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas estándar seguridad. En el contexto de este procedimiento, una inminente amenaza es definida como una situación en la cual la organización tiene evidencias para creer que un incidente de seguridad va a ocurrir.

- **Incidente de privacidad de la información:** Evento o serie de eventos no deseados e inesperados producto del tratamiento de los datos personales.
- **Incidentes de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000 2009].
- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).
- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Literal b, artículo. 6 de la Ley 1712 de 2014).
- **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 esta ley. (Literal c, artículo. 6 de la Ley 1712 de 2014).
- **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).
- **Ingeniería social:** Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social.
- **Inyección de ficheros remota**: Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web.
- **Inyección SQL:** Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos.
- **Incidente de seguridad digital - Ciberincidente:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008, o aquella que la modifique, adicione o sustituya.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014, o aquella que la modifique, adicione o sustituya.
- **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 y pseudominización
- **Modelo de Gobernanza de Seguridad digital:** Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país. (Decreto 338-2022).
- **Múltiples partes interesadas:** Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil.
- **NIST:** Es el Instituto Nacional de Estándares y Tecnología y busca promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.
- **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.
- **Pharming:** Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP (Internet Protocol) donde se aloja una web (página) falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.
- **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 27001:2022).
- **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).

- **Plan de Respuesta a Ciberincidentes:** Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, analizar, contener, erradicar y recuperar para minimizar las consecuencias de un ciberincidente.
- **Phishing:** Es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.
- **Plan de Continuidad de la operación:** Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- **Ransomware:** Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado, se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos, secuestrando computadores y servidores (imposibilidad de usarlo) o cifrando los archivos, con la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.
- **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 27001:2022).
- **Riesgo de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.
- **Rootkit:** Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo.
- **Scanner (Scanning) Escáner de vulnerabilidades:** Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.

- **Spam (correo basura):** Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de los usuarios que están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.
- **Spear Phising:** Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima).
- **Spyware "spy software":** Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.
- **Suplantación (Spoofing):** Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27001:2022).
- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades; que demanda la voluntad social y política de las múltiples partes interesadas. (Decreto 338 de 2022).
- **Suplantación de identidad:** Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.
- **Tecnologías de la Información - TI:** es el uso de computadoras, software, redes y otros equipos para recopilar, procesar, almacenar y transmitir datos e información. Incluye todo, desde el hardware y el software hasta la gestión de bases de datos y las redes de comunicación, como Internet.
- **Tecnologías de Operación:** La tecnología de operación se define como el conjunto de sistemas, procesos y herramientas que permiten a las empresas gestionar y controlar sus operaciones diarias de manera eficiente.
- **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 27001:2022).
- **Vulnerabilidad de seguridad digital:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización. (Decreto 338 de 2022).
- **Troyano:** Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.
- **Virus informático / malware / software malicioso:** Programa informático que está diseñado para realizar acciones maliciosas sobre un activo informático como copiarse a sí mismo, cifrar información, recolectar y filtrar información, entre otros, sin el consentimiento del propietario.

4. PROPÓSITOS DEL MSPI DEL AMB

- Definir los mecanismos y adoptar los lineamientos para adoptar el Modelo de Seguridad y Privacidad de la Información MSPI en el AMB.
- Desarrollar e implementar la estrategia de seguridad digital del AMB.
- Integrar la seguridad como habilitador en la política de Gobierno Digital mediante la definición de procedimientos.
- Contribuir a la transparencia en la gestión pública a través de la implementación efectiva del MSPI en el AMB.

5. MARCO JURÍDICO

Conforme con lo establecido en la normatividad vigente, basado en el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, se relacionan las siguientes normas, que se tienen en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

MARCO NORMATIVO
Constitución Política de Colombia Artículos 15, 209 y 269.
Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012 Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.
Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014 Por el cual se reglamenta el Registro Nacional de Bases de Datos.
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.
Decreto 103 de 2015 Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015 Por el que se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1080 de 2015 Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
Decreto 1081 de 2015 Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
Decreto 1083 de 2015 Por el cual se establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital.
Decreto 620 de 2020 Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad digital.

CONPES 4144 de 2025 Política Nacional de Inteligencia Artificial.
Decreto 728 de 2017 Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 1008 del 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 338 de 2022 Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3975 del 2019 Política nacional para la transformación digital e inteligencia artificial.
Ley 1915 de 2018 Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 612 de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
Decreto 767 de 2022 Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Norma ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
Decreto 1083 de 2015 Y sus modificaciones y actualizaciones.
Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1263 de 2022. Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI

El MSPI del Área Metropolitana de Barranquilla se basa en el ciclo del Modelo de Seguridad y Privacidad de la Información del MINTIC que contempla el siguiente ciclo de operación a través de cuatro (4) fases, las cuales permiten gestionar de manera óptima la seguridad y privacidad de los activos de información de la entidad partiendo inicialmente de un diagnóstico.

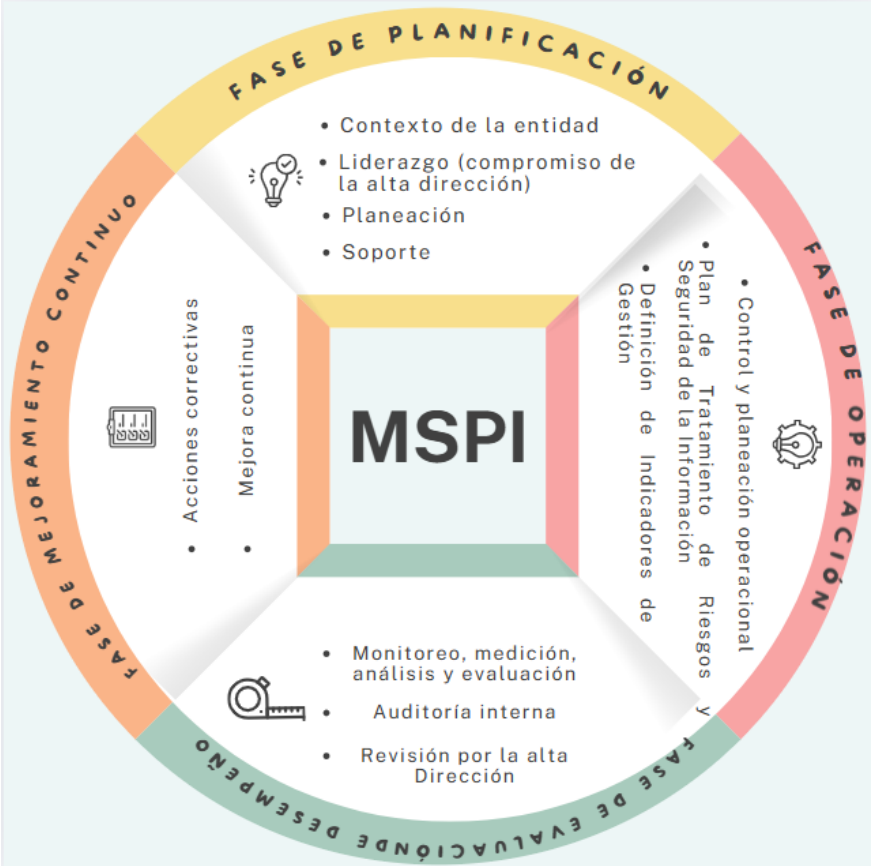


Figura1.Elaboración propia con base en la Ilustración 1. Ciclo del Modelo de Seguridad y Privacidad de la Información
Fuente: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

7. DIAGNÓSTICO

La elaboración del diagnóstico le permite a la entidad establecer el estado actual de la implementación de la seguridad y privacidad de la información, para esto se realiza el diligenciamiento de la herramienta dispuesta por el MINTIC, “Instrumento de evaluación MSPI” con el que se identifica de forma específica los controles implementados, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación.

El autodiagnóstico se realiza antes de la etapa de planificación y actualizar la información luego de terminar la fase de evaluación de desempeño, para identificar los cambios en el nivel de madurez de la implementación del modelo en la entidad, el resultado que se obtiene después de la evaluación de desempeño se toma como entrada en la fase de mejoramiento continuo.

Figura 2. Elaboración propia con base en la Ilustración 2. Ciclo del Modelo de Seguridad y Privacidad de la Información
Fuente: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

ESTADO ACTUAL DE LA ENTIDAD

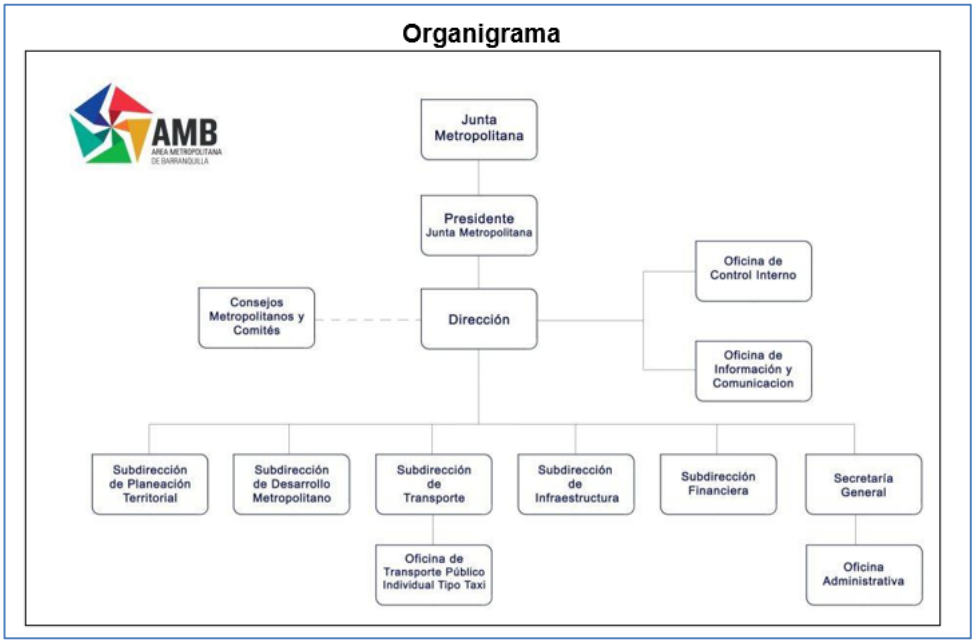
Contexto Institucional

Misión

Planeamos el desarrollo armónico del Área Metropolitana de Barranquilla mediante el ordenamiento territorial, la gestión del transporte público, la educación ambiental y la ejecución de obras, para mejorar la calidad de vida de nuestros habitantes y aumentar la competitividad de la región.

Visión

En el 2032 el Área Metropolitana de Barranquilla será una región competitiva, incluyente y sostenible, basada en la formación de una ciudadanía participativa, que impulse el desarrollo integral del territorio.



IDENTIFICACIÓN DEL NIVEL DE MADUREZ

Para identificar el nivel de madurez que tiene el Área Metropolitana de Barranquilla con respecto a la seguridad y privacidad de la información, se utilizó la herramienta ***"Instrumento de Evaluación MSPI de MINTIC",*** el cual arrojo el siguiente resultado:

Figura 3. Identificación del Nivel de madurez del AMB frente a la implementación del MSPI
Fuente: Instrumento de Evaluación MSPI de MINTIC.

LEVANTAMIENTO DE INFORMACIÓN

Partes interesadas / Stakeholders

El grupo de partes interesadas o stakeholders del AMB está conformado por los líderes de procesos que hacen parte del Comité Institucional de Gestión y Desempeño, a través del cual se toman las decisiones y/o se aprueban las decisiones que impacta a la entidad en materia de TI, el grupo de funcionarios, contratistas, terceros, empresas de transporte público y colectivo, proveedores y ciudadanía focalizada y general:

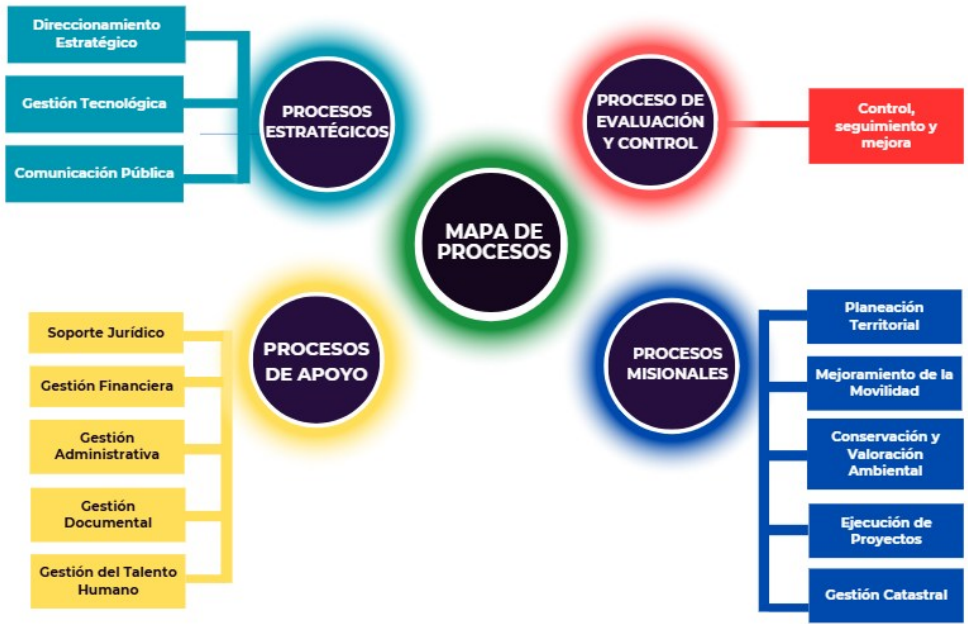
#	STAKEHOLDERS
1	Dirección
2	Secretaría General
3	Subdirección de Transporte
4	Subdirección de Planeación Territorial
5	Subdirección de Infraestructura
6	Subdirección de Desarrollo Metropolitano
7	Subdirección Financiera
8	Oficina Administrativa
9	Talento Humano
10	Comunicaciones
11	Oficina de Control Interno
12	Tecnología
13	Servidores públicos, contratistas y terceros que presten sus servicios o tengan alguna relación con la entidad a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio de información, interno o externo en el cumplimiento de los objetivos institucionales del Área Metropolitana de Barranquilla
14	Proveedores
15	Empresas de Transporte Público Colectivo e Individual
16	Ciudadanía del área metropolitana de Barranquilla
17	Ciudadanía de actualización y/o gestión catastral por convenios

Fuente propia OIYC AMB.

Mapa de Procesos

El mapa de procesos de la entidad conforme al actual Sistema de Gestión es el siguiente, el cual se clasifica en procesos estratégicos, misionales, de evaluación y control y procesos de apoyo.

En el mapa de procesos del sistema de gestión se incluyó el proceso de gestión catastral a pesar de no estar constituido por la estructura orgánica del AMB, pero se independizó del proceso de planeación territorial por el impacto y volumen que gestiona.



Fuente: Elaboración propia

8. FASE 1. DE PLANIFICACIÓN

La fase de planificación se basa en los resultados obtenidos en el instrumento de evaluación del MSPI, señalado en la fase anterior y el estado de la lista de chequeo de los documentos que sugiere la normatividad del MINTIC como producto en la fase de planeación del MSPI.

Lista de Verificación

Documentos Fase I. PLANIFICACIÓN MSPI

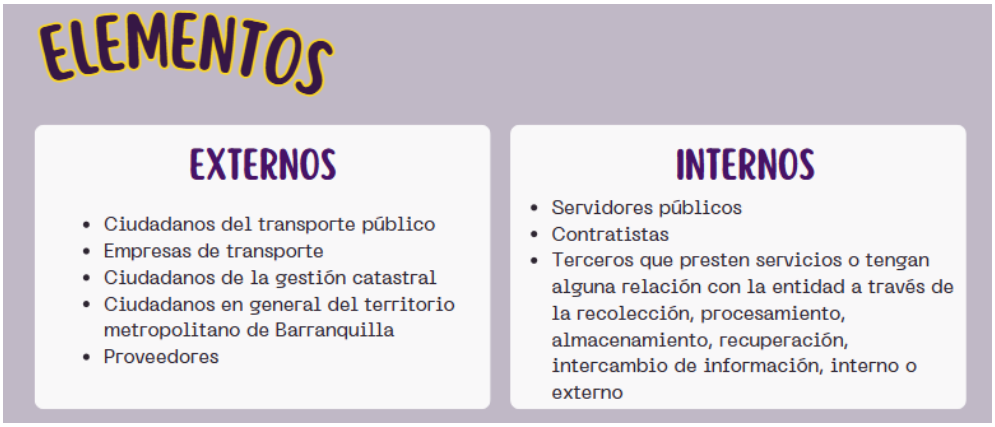
DOCUMENTO REQUERIDO:	SÍ	NO
Alcance MSPI.	✓	
Acto administrativo con las funciones de seguridad y privacidad de la información.	✓	
Adoptar la Política de seguridad y privacidad de la información mediante acto administrativo.	✓	
Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información.	✓	
Procedimiento de inventario y Clasificación de la Información e infraestructura crítica.		✗
Metodología de inventario y clasificación de la información e infraestructura crítica.		✗
Política de Gestión de Riesgos de la entidad con los lineamientos para la gestión de riesgos de seguridad y privacidad de la información	✓	
Plan de tratamiento de riesgos de seguridad de la información.	✓	
Declaración de aplicabilidad.	✓	
Manual de políticas de Seguridad de la Información.	✓	
Plan de Cambio, Cultura y Apropiación.		✗

Fuente: Elaboración propia

8.1. Contexto

8.1.1. Comprensión de la entidad y su contexto

Para determinar el contexto de la entidad, se identifican y detallan los elementos externos e internos que intervienen en ésta:



8.1.2. Necesidades y expectativas de los interesados

Con base en el análisis de los elementos externos e internos de la entidad (partes interesadas) que deben ser objeto de focalización del MSPI del AMB, a continuación, se relacionan las expectativas de cada uno de ellos frente a la seguridad de la información:

NECESIDADES / EXPECTATIVAS **PARTES INTERESADAS**

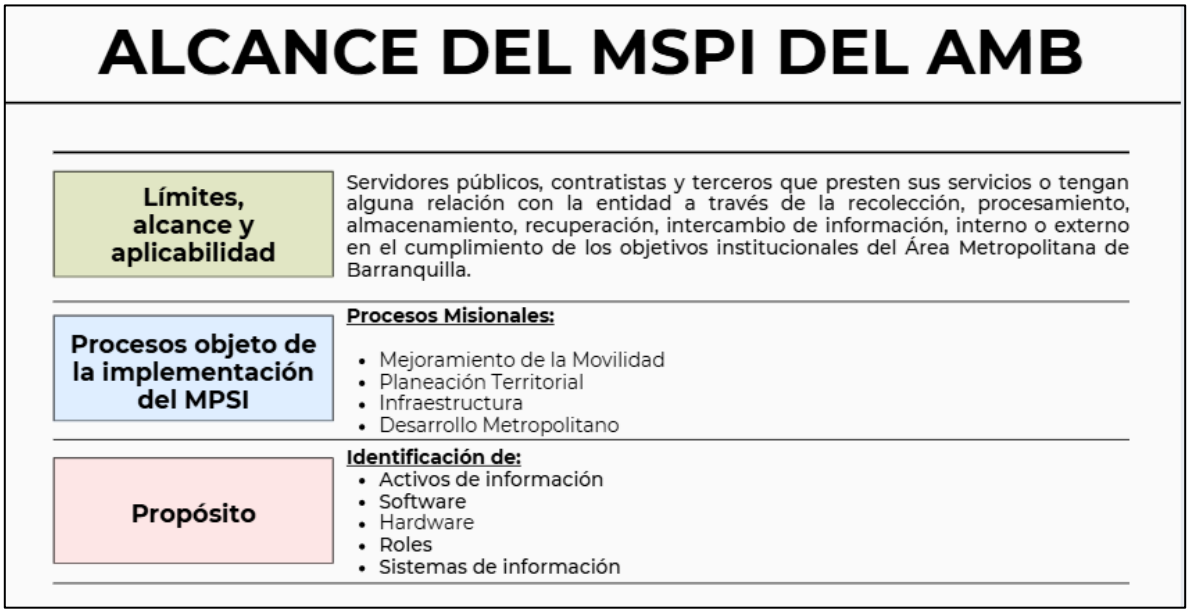
Partes Interesadas	Interno / Externo	Necesidad	Requisito	Expectativa
Usuarios del Transporte Público	EXT	Disponibilidad, integridad confidencialidad del Sistema de Recaudo, Control de flota e Información y comunicación al usuario.	Cumplimiento y seguimiento a la prestación del servicio del Aliado Tecnológico de la solución de Transporte público para el AMB.	• Recaudo Electrónico • Control de Floja • Comunicación en tiempo real
Empresas del Transporte Público	EXT	Disponibilidad, integridad y confidencialidad del Sistema de Recaudo y transacciones de pasajes.	Hacer seguimiento al cumplimiento de la efectividad del Sistema RCC para las Empresas de Transporte.	• Número de Transacciones efectuadas • Número de recargas efectuadas
Ciudadanos de la Gestión Catastral	EXT	Disponibilidad, integridad y confidencialidad del Sistema de Gestión Catastral de los municipios gestionados por la entidad.	Cumplimiento y seguimiento a la prestación del servicio de soporte y mantenimiento del Software de Gestión Catastral.	• Información catastral real y actualizada • Disponibilidad de la información.
Ciudadanos en General del AMB	EXT	Disponibilidad, integridad, confidencialidad y transparencia en la información que produce y entrega la entidad.	Disponibilidad, publicidad, transparencia de la información Institucional.	• Página web actualizada con la información mínima requerida • Optimización en la entrega de información requerida.
Proveedores	EXT	Disponibilidad y transparencia en los pliegos y/o especificaciones a contratar.	Definición, transparencia y cumplimiento de los términos y especificaciones de las necesidades a contratar.	• Transparencia en el proceso de selección de proveedores. • Integridad en la definición de condiciones.
Servidores Públicos	INT	Disponibilidad de la información.	Disponibilidad, confidencialidad e Integridad en la información suministrada para gestionar.	• Integridad, disponibilidad y confidencialidad de la información gestionada
Contratistas	INT	Disponibilidad de la información.	Disponibilidad, confidencialidad e Integridad en la información suministrada para gestionar.	• Integridad, disponibilidad y confidencialidad de la información gestionada
Terceros de OPS	INT	Disponibilidad de la información.	Disponibilidad, confidencialidad e Integridad en la información suministrada para gestionar.	• Integridad, disponibilidad y confidencialidad de la información gestionada

8.1.3. Definición del Alcance del MSPI

El alcance del Modelo de Seguridad y Privacidad de la Información del Área Metropolitana de Barranquilla, aplica para todos los procesos, servidores públicos, contratistas, terceros y comunidad focal del territorio, que en razón del cumplimiento de sus funciones, recolecten, procesen, almacenen, recuperen o intercambien información institucional, así como a los entes de control o entidades que accedan, ya sea, interna o externamente a cualquier tipo de información, indistintamente de la ubicación física que dispongan.

Enmarcado a proteger y preservar la integridad, confidencialidad, disponibilidad y transparencia de los activos de información de la entidad.

Gráficamente se establece el alcance del MSPI del AMB:



Fuente propia AMB. Alcance del MSPI.

8.2. Liderazgo

8.2.1. Liderazgo y Compromiso

El Área Metropolitana de Barranquilla, en cumplimiento de los lineamientos establecidos para definir y fortalecer los compromisos relacionados con la seguridad y privacidad de la información, y con el propósito de asegurar la adopción, implementación y mejora continua del MSPI de la entidad, dispone que el responsable de Seguridad y Privacidad de la Información del AMB participe como miembro invitado en las sesiones donde se aborden temas relacionados con la SPI. Asimismo, se designa al líder del proceso de gestión tecnológica como invitado permanente, con el fin de que éste comunique al encargado de la SPI los asuntos pertinentes tratados en las sesiones a las cuales no sea convocado directamente.

Se deja establecido entre las funciones del responsable del SPI las siguientes:

- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.

- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).
- Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.

8.2.2. Política de Seguridad y Privacidad de la Información

La entidad cuenta con una Política de Seguridad y Privacidad de la Información establecida, aprobada por el Comité Institucional de Gestión y Desempeño y adoptada a través de acto administrativo (resolución metropolitana), la cual se actualiza toda vez que sea necesario por cambios normativos externos y/o actualizaciones internas. En la Política se tienen en cuenta los lineamientos impartidos en materia de seguridad y privacidad de la información, estableciendo roles, responsabilidades, funciones, alcance y aplicabilidad.

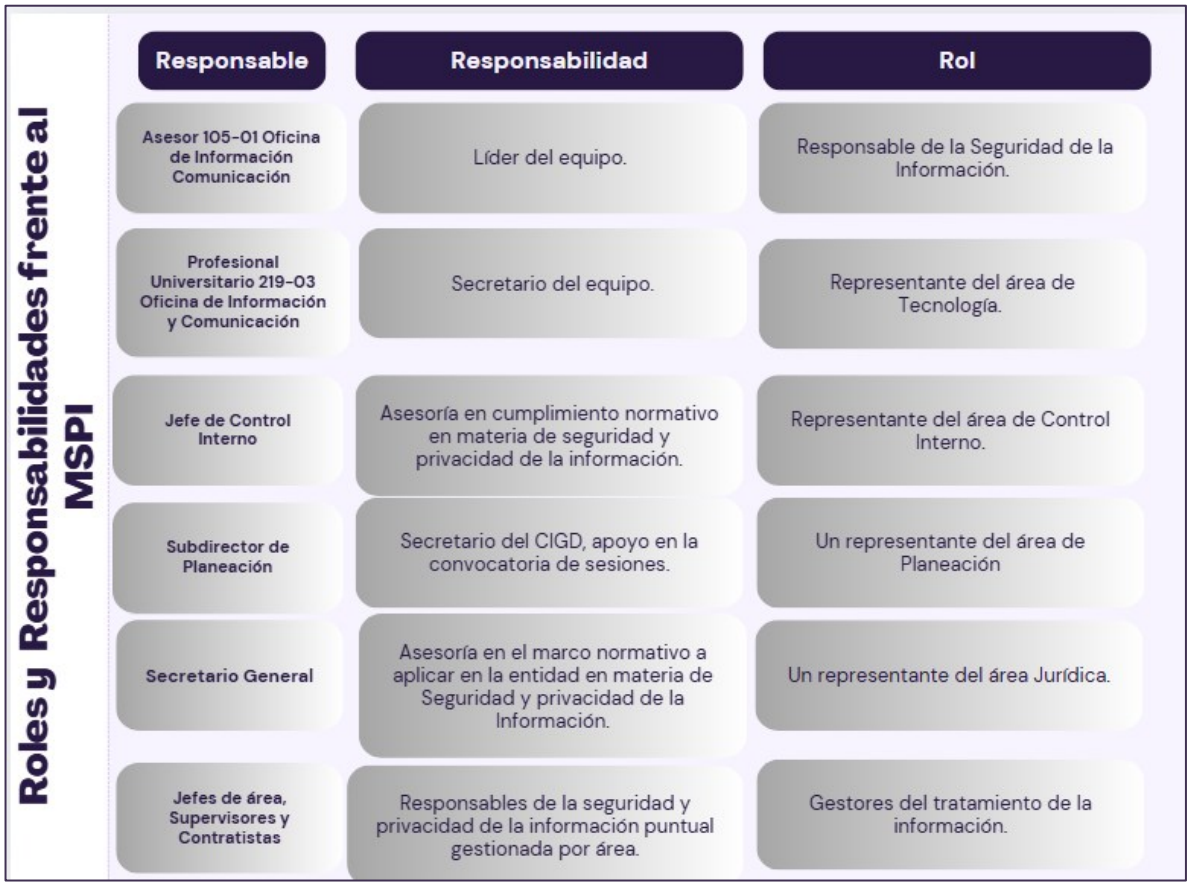
Se puede consultar la Política de Seguridad y Privacidad de la Información actual de la entidad en el siguiente link del sitio web oficial del AMB: https://www.ambq.gov.co/informacion-y-comunicacion/

8.2.3. Roles y responsabilidades del MSPI

Conforme a los lineamientos impartidos por el MINTIC la entidad define la confirmación del equipo de gestión del MSPI al interior de la entidad, estableciendo los roles, responsables y responsabilidades de cada uno frente a la adopción del Modelo.

- **Identificación de los responsables:**

Los representantes del nivel directivo de la entidad identifican y establecen, sin perjuicio de lo establecido en la Ley 489 de 1998, la conformación del equipo de trabajo responsable para implementar el MSPI del AMB, definiendo el responsable. Teniendo en cuenta lo anterior, al final del ejercicio el equipo directivo que lidera la implementación del MSPI, se obtiene la siguiente matriz del equipo de trabajo:



Fuente propia. Roles y responsabilidades frente al MSPI – AMB.

- **Responsable de Seguridad de la Información para la entidad:**

El responsable de Seguridad de la información es el líder del proyecto y tendrá las siguientes responsabilidades:

- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- Implementación del Modelo de Seguridad y privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos.
- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

8.3. Planeación

8.3.1. Identificación de activos de información e infraestructura critica cibernética

La entidad conforme a los lineamientos establecidos por el MINTIC para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional Ministerio de tecnologías de la información y las comunicaciones MSPI, identifica y tipifica sus activos de información de acuerdo con las directrices del Archivo General de la Nación, que implementan la metodología apropiada sobre el tratamiento de los “tipos de información y documentos físicos y electrónicos, así como los sistemas, medios y controles asociados a la gestión”.

Los propietarios y custodios de la información producida por cada una de las áreas, identifican, clasifican y valoran los activos de información de acuerdo con la siguiente compilación de Activos de Información teniendo en cuenta lo establecido en la norma técnica ISO/IEC 27001:2022 (Información; Software como programa informático; Hardware como computadora; servicios; personas, y sus calificaciones, habilidades y experiencia; intangibles como reputación e imagen), con el acompañamiento del área de gestión documental y tecnología de la información. Tomando como base las Tablas de Retención Documental - TRD de la entidad.

Para llevar a cabo la identificación de los activos de información, el AMB parte de los siguientes conceptos:

Información básica: hace referencia a aquellas características mínimas del activo que deben identificarse durante esta fase:

- **Macroproceso:** Macroproceso de la Entidad al que pertenece el activo de información (En caso de que existan).
- **Proceso:** Proceso de la Entidad al que pertenece el activo de información.
- **Identificador:** Se sugiere que el identificador sea una concatenación del código de la dependencia según la Tabla de Retención Documental (TRD) + número consecutivo.
- **Tipo:** Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

Tipificación del activo	Descripción	Componentes	Activo de Información AMB
Información	Corresponden a este tipo datos e información almacenada o procesada electrónicamente.	Tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de	▪ Base de Datos Sistema de Nómina y Financiero. ▪ Base de Datos Sistema de trámites de transporte público e individual.

		confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.	▪ Base de Datos de la flota, recaudo e información al usuario. ▪ Base de Datos de la correspondencia recibida y generada de la entidad. ▪ Base de Datos de la gestión catastral de los municipios gestionados por el AMB. ▪ Enlace a SECOP II de información contractual de la entidad. ▪ Documentación del Sistema de Gestión de la entidad.
Hardware	Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la entidad.	Servidores, routers, módems Computadores (portátiles, escritorio), impresoras, Celulares Tablet, Teléfonos IP	▪ Servidores **(3)** ▪ Routers **(7)** ▪ Switch **(6)** ▪ Firewall **(2)** ▪ GPS **(11)** ▪ UPS **(1)** ▪ Computadores de escritorio **(129)** ▪ Computadores portátiles **(19)** ▪ Impresoras **(30)** ▪ Escáneres **(21)** ▪ Proyectores **(5)** ▪ Granjas de Control de tráfico **(2)** ▪ DVR **(2)**
Software	Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la entidad y la prestación de los servicios.	Software de aplicación, correo electrónico, sistema operativo, etc.	▪ Software de Nómina y Financiero ▪ Software de trámites de transporte público e individual ▪ Software de gestión de flota, recaudo e información al usuario ▪ Software de gestión documental ▪ Software de gestión catastral ▪ G-Suite de Google para la administración de cuentas de correo electrónico institucional ▪ Sistema Operativo Windows Server ▪ Sistema Operativo Windows 11 ▪ Licencias de Office 365 ▪ Sistema de protección antivirus
Servicios	Servicios de computación y comunicaciones.	Tales como Internet, páginas de consulta, directorios compartidos e Intranet.	▪ Canal dedicado de fibra óptica para conexión a Internet ▪ C-panel y Página web de la entidad ▪ Directorio activo
Recurso Humano	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso,	Contratistas, funcionarios, proveedores.	▪ Servidores públicos **(79)** ▪ Contratistas **(292)**

	son consideradas activos de información.		
Instalaciones	Los lugares donde se almacenan o resguardan los sistemas de información y comunicaciones.	Centros de cómputo, centros de cableado, Datacenter.	▪ Centro de datos y centro de cableado Piso 1. Cra 46 # 82–209. ▪ Centro de datos y centro de cableado Piso 4. Cra 46 # 82 – 209. ▪ Colacation 6 unidades de rack.
Infraestructura crítica cibernética Nacional	Se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado.	Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.	▪ Sistema de trámites de Transporte Colectivo e Individual y su Base de Datos. ▪ Sistema de Gestión Catastral y su Base de Datos.

Tabla 1 Tipificación de Activos. Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional Ministerio de tecnologías de la información y las comunicaciones

- **Serie documental:** Serie documental del área, dependencia o proceso que se encuentra identificando el Activo.
- **Subserie documental:** Subserie documental del área, dependencia o proceso que se encuentra identificando el Activo.
- **Nombre:** Nombre completo del activo de información.
- **Descripción:** Descripción resumida de manera clara para identificar el activo de información.
- **Nombre del responsable de la producción de la información (Propietario del activo):** Nombre del área, dependencia, proceso responsable de producir el activo de información.
- **Fecha de generación de la información:** Fecha en la que el activo de información fue incluido en el inventario de activos de información.
- **Custodio del activo de la información:** Corresponde al nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección**.**
- **Fecha de ingreso del activo al archivo:** Fecha en la que el activo ingresa al archivo de gestión. (Aplica para los activos tipo información)
- **Soporte de registro: De acuerdo con el Decreto 2609 de 2012: o Físico (análogo):** Este campo se diligencia si el Tipo de activo es "Información" o Digital o Electrónico; Este campo se diligencia si el Tipo de activo es "Información" o N/A: Para el resto de los tipos de activos se debe seleccionar N/A.
- **Medio de conservación:** De acuerdo con el Decreto 2609 de 2012 Archivo Institucional Es la instancia administrativa de custodiar, organizar y proteger.

- **Formato:** Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: Hoja de cálculo, imagen, audio, video, documento de texto, etc.
- **Idioma:** Establece el idioma, lengua o dialecto en que se encuentra la información.

Con base en lo anterior, la entidad clasifica los activos de información de acuerdo con la confidencialidad, integridad y disponibilidad y lo dispone en el sitio web oficial: https://www.ambq.gov.co/informacion-y-comunicacion/

8.3.2. Valoración de los riesgos de Seguridad de la Información

La entidad identifica y valora los riesgos de seguridad de la información y los dispone en el Sistema de Gestión:

Fuente propia AMB.

8.3.3. Plan de Tratamiento de los riesgos de Seguridad de la Información

La entidad cuenta con un Plan de Tratamiento de riesgos de Seguridad de la Información establecido, aprobada por el Comité Institucional de Gestión y Desempeño y adoptada a través de acto administrativo (resolución metropolitana), la cual se actualiza toda vez que sea necesario por cambios normativos externos y/o actualizaciones internas.

En dicho plan se tienen en cuenta los lineamientos impartidos en materia de riesgos de seguridad de la información y puede ser consultado en el siguiente link del sitio web oficial del AMB: https://www.ambq.gov.co/informacion-y-comunicacion/

8.4. Soporte

8.4.1. Recursos

Con el fin de establecer y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI, el AMB determina que en la actualidad con el personal de planta vinculado se logran desarrollar las actividades para la adopción, implementación, mantenimiento y mejora continua del MSPI, así como las actualizaciones relacionadas con el Plan Estratégico de Tecnología de la Información – PETI.

8.4.2. Competencia, toma de conciencia y comunicación

Con el Plan de Comunicaciones para el MSPI en el Área Metropolitana de Barranquilla se pretende no solo transmitir información, sino, lograr la adopción de los nuevos conocimientos, hasta convertirlos en la aplicación de mejores prácticas de manera frecuente, de tal manera que se logre un mejoramiento continuo en la entidad.

Lo anterior, con el fin de instruir, verificar y validar el accionar de los usuarios, en función del MSPI definido.

- **Políticas Corporativas (institucionales):** Los usuarios deben comprender las políticas de seguridad de información establecidas por la entidad para evitar los incumplimientos no intencionales a éstas.

- **Aspectos de seguridad:** Se requiere entrenar a los empleados en diferentes aspectos de seguridad, desde acceso físico, mal uso de la información, seguridad en el correo electrónico, etc., buscando que apoyen con su comportamiento las diferentes iniciativas de seguridad que se desarrollen.

- **Rol del usuario (servidor público, contratista, tercero):** Las personas tienden a prestar menos atención a aspectos que no los afectan directamente. El comportamiento adecuado y las acciones proactivas son más probables si los empleados entienden las consecuencias negativas para la organización y para ellos mismos de no acatar las diferentes políticas de seguridad.

Con base en los principios de la seguridad de la información, la entidad define el siguiente Plan de Comunicación del MSPI para el AMB:

PLAN DE COMUNICACIÓN DEL MSPI

OBJETIVO	QUÉ COMUNICA	FRECUENCIA	ESTRATEGIA	A QUIEN COMUNICA
Dar a conocer el uso y los beneficios que plantea el Gobierno nacional con la iniciativa de datos abiertos.	Oficina de Información y Comunicación.	SEMESTRAL	• Redes sociales Internas • Correo Institucional	Toda la comunidad del AMB
Dar a conocer la ley 1712 de 2014 Transparencia y acceso a la Información pública con el fin de generar un cultura de transparencia, legalidad e Integridad en el AMB.	Subdirección de Planeación. Oficina de Información y Comunicación.	SEMESTRAL	• Redes sociales Internas • Correo Institucional	Toda la comunidad del AMB
Socializar los lineamientos del proceso Gestión Tecnológica.	Oficina de Información y Comunicación.	SEMESTRAL	• Grupo de Whatsapp del AMB • Correo Institucional	Toda la comunidad del AMB
Campaña de sensibilización en materia de seguridad de la información a nivel interno de la entidad.	Oficina de Información y Comunicación.	CUATRIMESTRAL	• Grupo de Whatsapp del AMB • Correo Institucional	Toda la comunidad del AMB

Fuente propia OIYC AMB.

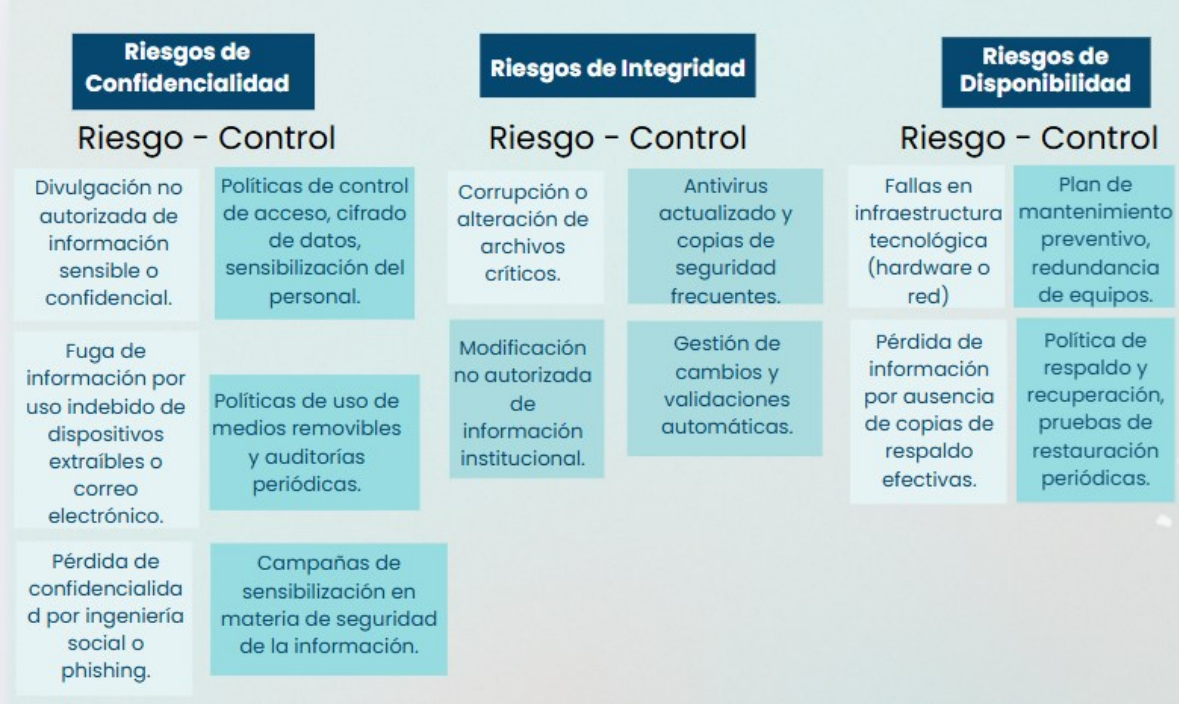
9. FASE 2. DE OPERACIÓN

Como desarrollo de la fase de operación, la entidad planifica la implementación y aplicación de controles a los procesos necesarios para cumplir los objetivos y requisitos de seguridad y con el fin de llevar a cabo la valoración y tratamiento de riesgos de la seguridad de la información establecidos previamente.

9.1.1. Control y Planeación operacional

Con el fin de llevar a la implementación de las acciones determinadas en el Plan de Tratamiento de Riesgos y el Plan de Seguridad y Privacidad de la Información, la entidad documenta adopta los lineamientos en materia de seguridad de la información, aprobados por el Comité Institucional de Gestión de Desempeño y establece los planes y controles para lograr los objetivos del MSPI.

Los controles se documentan, gestionan y se hacen seguimiento a través del Sistema de gestión de la entidad.



Fuente propia OIYC AMB.

9.1.2. Plan de Tratamiento de riesgos

La entidad define y gestiona la Matriz de riesgos de seguridad de la información mediante del Sistema de Gestión y el Plan de Seguridad de la Información, se encuentra disponible en el sitio web oficial del AMB: https://www.ambq.gov.co/informacion-y-comunicacion/

9.1.3. Definición de Indicadores de gestión

Los indicadores de Seguridad de la Información del Área Metropolitana de Barranquilla se utilizan para evaluar su desempeño y eficacia.

La medición queda registrada en la herramienta o formato establecido por la Oficina de Control Interno en el Sistema de Gestión de la entidad.

10. FASE 3. DE EVALUACIÓN Y DESEMPEÑO

10.1.1. Seguimiento, medición, análisis y evaluación

- ❖ Seguimiento:

Como medidas de seguimiento al MSPI, se define en este modelo el desarrollo de las siguientes actividades:

- Revisiones por parte del Líder del proceso al alcance del MSPI y proponer en caso de aplicar, mejoras y/o actualizaciones de este.
- Revisión y actualizaciones a los Planes de seguridad, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en esta fase del SGSI.

- ❖ Medición:

Se establecen las siguientes actividades generales para soportar la etapa de medición del MSPI:

- Medición de la efectividad de Controles.
- Revisión de las valoraciones de los riesgos.
- Medición de los indicadores de gestión del MSPI.
- Actualizar los planes de seguridad.
- Registro de los incidentes del MSPI en caso de aplicar.
- Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).
- Medición:

- ❖ Análisis y evaluación:

Se establecen las siguientes actividades generales para soportar el desarrollo es esta etapa:

- Semestralmente hacer seguimiento a los indicadores de gestión establecidos
- Evaluar indicadores frente a las metas
- Presentar los Indicadores al área encargada del sistema de gestión en la entidad
- Evaluar las No Conformidades ocurridas y su impacto en el cumplimiento de las metas y objetivos del MSPI, en la eventualidad de que se lleguen a presentar.

10.1.2. Auditoría interna

La auditoría interna definida por la entidad para obtener información sobre el cumplimiento del MSPI se llevará a cabo como medida de autocontrol del proceso de gestión tecnológica anualmente, con la utilización de herramientas y lineamientos establecidos por el MINTIC y

adicionalmente, auditorías internas aplicadas por la Oficina de Control interno del AMB, cuando ésta lo establezca en su Plan de Auditoría.

10.1.3. Revisión por para de la Dirección

La documentación del MSPI y su seguimiento serán revisados por la alta dirección y se dejará acta de constancia con los compromisos a los que haya a lugar.

11. FASE 4. MEJORAMIENTO CONTINUO

11.1.1. Mejora continua y Acciones correctivas y No conformidades

Con base en los seguimientos, revisiones y auditorias aplicadas al Modelo de Seguridad y Privacidad de la Información del AMB, se estructuran un plan de anual de mejora del MSPI que incluya los controles de seguridad a implementar, oportunidades de mejora, no conformidades y demás actividades encaminadas a la gestión de los procesos de seguridad de la información.