FONDO MUNICIPAL DE TRÁNSITO Y TRANSPORTE TERRESTRE MAGANGUÉ

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN 2026

SECRETARÍA GENERAL – PROFESIONAL DE APOYO

GINA MENCO ROJAS

DIRECTORA

Magangué, enero de 2026

INTRODUCCIÓN

El Plan de Privacidad y Seguridad de la Información del Fondo de Tránsito y Transporte de Magangué, Bolívar, establece los elementos fundamentales para preservar la confidencialidad, integridad y disponibilidad de la información, y determina los procesos, procedimientos y controles que se deben aplicar conforme a la legislación colombiana y a los requerimientos y objetivos estratégicos de la entidad. El logro de este, facilita el cumplimiento de las políticas, aquí definidas y brinda las herramientas necesarias para que los funcionarios, contratistas y terceros que hacen parte del SGSI, puedan adoptar los controles requeridos y asegurar la información, gestionar con eficiencia los riesgos de seguridad y obtener mejoras continuas. La información es dinámica y cambiante, por ende, toda entidad pública o privada debe articular entre el SGSI y las políticas de seguridad de la información, esto se logra integrando las políticas, procedimientos, sistemas de información y controles, con el fin de gestionar, de manera pertinente y eficaz, los riesgos, de tal forma que se obtengan altos niveles de seguridad y confianza; estas políticas deben ser plenamente conocidas y cumplidas por los funcionarios, contratistas y terceros que tienen acceso a los activos de información y a los sistemas de procesamiento de información.

Actualmente Colombia viene adelantando la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2; como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, esto se ha articulado al Modelo Integrado de Planeación y Gestión-MIPG, como herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, unida a otras políticas esenciales para la gestión pública.

Existe un Manual de Política de Gobierno Digital, expedido por MINTIC, que establece una política, cuyo propósito promueve el uso y aprovechamiento de las TICS, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Según el manual, la implementación de la política de Gobierno Digital se ha definido en dos componentes: TIC para el Estado y TIC para la sociedad, con tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Todos estos elementos, se desarrollan a través de lineamientos y estándares que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información,

infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información –MSPI-. El documento denominado Modelo de Seguridad y Privacidad de la Información – MSPI, expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción del mismo, por las entidades del Estado, conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2., en el numeral 2, en los literales A, B y C, el cual debe ser planificado en atención a lo establecido en el decreto 612 de 2018, que en el artículo 1 señala la importancia de la integración de los planes institucionales y estratégicos al Plan de Acción institucional, en el ámbito de aplicación del modelo integrado de planeación y gestión.

1. OBJETIVOS.

1.1. Objetivo General.

Establecer un marco de acción para la implementación del Modelo de Seguridad y Privacidad de la Información, en atención al contexto organizacional del Organismo, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios, socios y demás partes interesadas del Fondo.

1.2. Objetivos Específicos.

- ✓ Contribuir a mejorar los procesos de intercambio de información pública del Fondo.
- ✓ Orientar al Fondo en las mejores prácticas en seguridad y privacidad.
- ✓ Optimizar la gestión de la seguridad de la información al interior del Fondo.
- ✓ Contribuir al incremento de la transparencia en la gestión pública.
- ✓ Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- ✓ Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en El Fondo.
- ✓ Orientar en El fondo, la transición de lPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
- ✓ Orientar en El Fondo, la adopción de la legislación relacionada con la protección de datos personales.
- ✓ Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- ✓ Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del Fondo.
- ✓ Orientar al Fondo en mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- ✓ Revisar los roles relacionados con la privacidad y seguridad de la información al interior del Fondo, para optimizar su articulación.

2. ALCANCES E IMPORTANCIA.

La adopción del Modelo de Seguridad y Privacidad de la Información, para la vigencia 2026, se enfocará en fortalecer la implementación de acciones, acorde a los lineamientos emitidos por el MINTICS, orientados a la seguridad informática de la plataforma e infraestructura tecnológica del Fondo, teniendo en cuenta las capacidades y recursos disponibles para mejorar la confianza de los ciudadanos, usuarios internos, externos y ciudadanía en general.

El Plan de Seguridad y Privacidad de la Información, considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos del Organismo, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea, a fin de precisar la estrategia de ejecución de los controles de seguridad requeridos. Mediante el aprovechamiento de las TICS y el modelo de seguridad y privacidad de la información, se fortalece la seguridad de la información, se garantiza la protección de la misma y la privacidad de datos de ciudadanos y funcionarios, todo, según lo expresado en la legislación colombiana. El Plan y su política, se aplica a los funcionarios, sus recursos, procesos y procedimientos internos y externos, igual al personal vinculado y terceros, que usen activos de información que sean propios.

Finalmente, La información se considera un activo fundamental y cumple rol vital para El fondo. Es el oxígeno para el organismo: Debe fluir adecuada y oportunamente a todas las áreas. Evitar filtraciones hacia asuntos diferentes, entre otros riesgos. Un buen Sistema de Gestión de Seguridad de la Información (SGSI) ayuda a gestionar y proteger la información. Preservar la confidencialidad, la integridad y la disponibilidad de la información es la base para erigir la seguridad de la información, la cual debe ser:

Confidencialidad: Un SGSI garantiza que la información de la organización no estará disponible, ni será revelada a personas, organizaciones o procesos no autorizados.

Integridad: El SGSI promete mantener la información exacta y completa, tal como fue finalmente elaborada, así como sus métodos de proceso.

Disponibilidad: Las personas, organizaciones y procesos que tengan acceso autorizado a la información deberán disponer de ella cuando la requieran.

Entre los beneficios que tiene, quién implemente un SGSI, tenemos: disminución del impacto de los riesgos; mayores garantías de continuidad del negocio basadas en la adopción de un plan de contingencias; mejora la imagen de la organización y aumenta el valor comercial y los servicios; una mayor confianza por parte de clientes, proveedores, clientes y socios; una mejora de las inversiones; el cumplimiento de la legislación y normativa vigentes, etc.

3. MARCO NORMATIVO.

NORMA	AÑO	DESCRIPCIÓN
Políticas técnicas de seguridad de la información Función Pública.	2020	La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades
Decreto 103 de 2015.	2019	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015.	2019	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1008 de 2018.	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2018.	2018	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea
Decreto 2573 de 2018.	2018	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 1377 de 2013.	2018	Decreto 1377 de 2018 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	2017	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012.	2017	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011.	2017	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011.	2017	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1273 de 2009	2016	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

Ley 527 de 1999	2015	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Constitución Política de Colombia. 1991, Artículo 15.	2013	Todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, y El estado debe respetarlos y hacerlos respetar.
Ley 23 de 1982	2015	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Norma técnica colombiana NTC-ISO/IEC 27001 DE 2013	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581 de 2012.	2012	Ley 1581 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 57 de 1985	1985	Publicidad de los actos y documentos oficiales.
Decreto Ley 2150 de 1995	1995	Supresión y reformas a regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
Ley 594 de 2000.	2000	Ley General de Archivos.
Decreto 1747 d3 2000	2000	Entidades de certificación, los certificados y las firmas digitales.
Ley 962 d3 2005.	2005	Racionalización de trámites y procedimientos administrativos procedimientos administrativos.
Ley 1266 de 2008.	2008	Disposiciones generales de habeas data y se regula el manejo de la información.
Ley 1437 de 2011.	2011	Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
Decreto 2364 de 2012.	2012	Firma electronica.
Ley Estatutaria 1757 de 2015.	2015	Promoción y protección del derecho a la participación democrática.
Acuerdo 03 de 2015	2015	Archivo General de la Nación - Lineamientos generales sobre la gestión de documentos electrónicos.

4. MARCO CONCEPTUAL.

El glosario de términos y conceptos en este Plan son:

- **Riesgo de seguridad de la información:** Posibilidad que una amenaza concreta, pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; los daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que genera. También se genera riesgo positivo en la seguridad de información por aprovechamiento de oportunidades y fortalezas presentados.
- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- **Seguridad de la Información**. Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos**: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literalh).
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles**: Datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación,

tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad**: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad**: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008. • Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos:** Directorio público de 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).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que usa una organización para fijar una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. DIAGNÓSTICO SITUACIÓN ACTUAL.

5.1. Política de Seguridad Informática.

La política de seguridad informática se establece en El Organismo, acorde con lo planteado por El Gobierno nacional, en cumplimiento a las actividades desarrolladas en la implementación del Modelo de Seguridad y Privacidad de la Información-MSPI, debiendo tener en cuenta las políticas específicas que describimos a continuación:

5.1.1. Política de roles y responsabilidades.

Hacer buen uso de la información que es generada resultado de las actividades laborales. Se debe definir los roles, responsabilidades y competencias en seguridad de la información. En El Organismo, todos los usuarios somos responsables de la información automatizada que manejamos y damos estricto cumplimiento a los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Se debe capacitar a todos los Colaboradores y terceros solicitantes de accesos a componentes tecnológicos y sistemas de información sobre el uso y la responsabilidad que tienen al ser autorizados. Igualmente, hacer una matriz de roles y responsabilidades en seguridad de la información, la cual debe ser actualizada periódicamente o cada vez que se requiera.

5.1.2. Política de dispositivos móviles.

Se debe llevar un registro y control de todos los dispositivos móviles que posee la Entidad. Se debe hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales. Se debe definir un procedimiento de formal de salida de dispositivos.

Todos los servidores y colaboradores del organismo son responsables de garantizar el buen uso de los dispositivos móviles en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

5.1.3. Política de seguridad de los recursos humanos.

El Objetivo es garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja para El Fondo, a través de mecanismos de validación y concientización del recurso humano que hará uso de esta.

Se debe incorporar la Seguridad en la matriz de Cargos de la entidad, el Control y Política del Personal, los Acuerdos de Confidencialidad, adecuada selección de personal, de los Términos y condiciones Laborales, del Entrenamiento,

concientización y capacitación, Formación y Capacitación en Materia de Seguridad de la Información y del manejo de Procesos disciplinarios.

5.1.4. Política de uso de correo electrónico.

El Objetivo es definir las directrices generales del buen uso del correo electrónico en El Organismo. El uso aceptable del servicio, implica que, se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en el Ministerio y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen del Fondo. Todos los servidores y colaboradores, que sean autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus acciones de acceso al correo. Además, se debe dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información del Fondo. En síntesis, se debe evitar el uso no aceptable o incorrecto del servicio o para fines personales.

5.1.5. Política de uso de internet.

El objetivo es definir la política de buen uso del internet, con el fin de asegurar una adecuada protección de la información del Fondo. El Uso aceptable del servicio, implica su utilización exclusiva para el desempeño de las funciones y actividades desarrolladas durante el desempeño de funciones y no debe utilizarse para ningún otro fin.

Las personas autorizadas para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos del Fondo, o que afecte la seguridad de la información de éste. Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control. En igual forma, se debe evitar el uso no aceptable o incorrecto del servicio o para fines personales.

5.1.6. Política de uso de redes sociales.

El objetivo es decidir la política para el uso del servicio de Redes sociales por parte de las personas autorizadas en El Fondo. El uso aceptable del servicio, debe asegurar un uso exclusivo para el desempeño de funciones y actividades propias del desempeño de funciones y no debe utilizarse para ningún otro fin.

Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información del Fondo. El facilita el acceso a estas

herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar por parte de los servidores y colaboradores, sin embargo, es necesario hacer buen uso de forma correcta y moderada.

5.1.7. Política de uso de recursos tecnológicos.

El objetivo es decidir la política para el uso aceptable de los recursos tecnológicos del Fondo. El uso conforme de los recursos tecnológicos del Fondo precisa, tenerlos como elementos necesarios y como como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los servidores y colaboradores y no para fines distintos.

Es en consideración a lo anterior que, el uso debido de estos recursos es de exclusiva responsabilidad de los usuarios, los cuales deberán asegurarse de que estos no contengan ningún medio de contaminación de virus o que con sus acciones y uso los deterioren o afecten su funcionamiento. Los equipos de cómputo suministrados por El Fondo, se deben entregarán mediante un acta de entrega, en donde se detalle sus elementos constitutivos y a quién se le entregue responderá por éste.

5.1.8. Política de Telefonía y dispositivos móviles.

Objetivo es asegurar que los teléfonos móviles se deben utilizar exclusivamente para desempeñar funciones asignadas al cargo dentro del Fondo. La Entidad se reserva el derecho de revisar la utilización del dispositivo telefónico ante cualquier sospecha de un uso inapropiado del mismo.

5.1.9. Política de uso del Software legal y Derechos de Autor.

Objetivo es asegurar que, los usuarios solo podrán utilizar software legalmente adquirido y/o autorizado por El Fondo. En caso de presentarse algún tipo de reclamación por software ilegal, esta recaerá sobre el usuario responsable en donde se encontrase instalado dicho software; debido a que está atentando contra los derechos de autor.

En presentaciones, documentos, informes y demás documentos que utilicen los usuarios para funciones de su cargo, debe mencionarse la fuente de donde se extrajo la información. Los usuarios no pueden realizar copias de software que se encuentre instalado o sea desarrollado por el Fondo, para su distribución.

5.1.10. Política de Acceso Inalámbrico.

Su objetivo es asegurar que, el uso de la red inalámbrica será exclusivo para usuarios de planta y contratistas con vínculo directo con El Fondo, se habilitará el servicio previa solicitud, justificación y autorización a la Dirección o el funcionario competente. Para accesos a dispositivos móviles, se realizará solo previa solicitud y justificación a la Dirección General.

5.1.11. Política de clasificación de la información.

El objetivo es asegurar que la información del Fondo, sea tratada y protegida adecuadamente. Esta se debe identificar y clasificar, etiquetear y manejar adecuadamente. El uso no conforme de ella, tal como omisión, retardos o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos, solicitudes y denuncias, de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web. Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo. Divulgación no autorizada de los expedientes, documentos, información o archivo.

Realizar actividades tales como borrar, modificar, alterar o eliminar información del Ministerio de manera malintencionada, dará lugar a las acciones legales o judiciales pertinentes por parte del Organismo.

5.1.12. Política de gestión de almacenamiento.

Objetivo es Proteger la información del Fondo, velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento. Se restringe el uso de información compartida, en cualquier forma o método. Si el colaborador no adopta controles y no se hace responsable de la pérdida o infiltración de la información, asumirá las consecuencias legales.

Por lo anterior deberá gestionar y Disponer de medios removibles para almacenamiento, de borrado seguro y de transferencia e medios físicos.

5.1.13. Política de Control de Acceso.

Su objetivo es Definir las directrices generales para un acceso controlado a la información del Fondo. Por lo tanto, en El Organismo, se tendrá Control de Acceso a Redes y Servicios en Red, a la gestión de acceso de usuarios, a la revisión de los derechos de acceso de usuarios y al retiro de derechos de acceso de usuarios.

5.1.14. Política de Seguridad Física y del entorno.

Objetivo es evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información del Fondo. Es así que se debe establecer perímetro de seguridad física, control de acceso físico, ubicación y protección de equipos, seguridad de equipos por fuera de instalaciones, seguridad en la reutilización o eliminación de equipos y retiro de equipos y activos.

5.1.15. Política de escritorio y pantalla despejada.

Objetivo es Objetivo definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información del Fondo. Todo el personal del debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

5.1.16. Política de gestión de cambios.

El objetivo es asegurar que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en El fondo, se realicen de forma controlada. Se deben establecer procedimientos para el control de cambios ejecutados en El Organismo. Toda solicitud de cambio en los servicios de infraestructura y sistemas de información del Fondo, se debe realizar siguiendo el Procedimiento de gestión de cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información. Se debe llevar una trazabilidad del control de cambios solicitados.

5.1.17. Política de separación de ambientes de desarrollo, pruebas y producción.

El objetivo es reducir riesgos asociados a modificaciones, alteraciones, cambios o accesos no autorizados en sistemas en producción del Fondo. Se debe establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información del Organismo. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario y clasificación de activos de información.

En El fondo se debe seguir un procedimiento formal para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (desarrollo, pruebas y producción), se debe establecer una guía para el Desarrollo seguro de Software.

5.1.18. Política de protección contra código malicioso.

El objetivo, definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en El fondo. Toda la infraestructura de procesamiento de información debe contar con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

5.1.19. Política de backup.

El objetivo, proporcionar medios de respaldo de información adecuados en El Organismo, para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla. Es por esto que se debe contar con: Registro de Respaldo de Información y Respaldo de información para usuarios finales.

Es responsabilidad todos los servidores y Terceros almacenar la información crítica asociada con su labor en el servidor de archivos establecido, para garantizar que la información está siendo respaldada.

5.1.20. Política de eventos de auditoría.

El objetivo, asegurar que los registros de los eventos y las operaciones realizadas sobre los sistemas de información y plataforma tecnología del Fondo permitan contar con evidencia necesaria para la gestión de incidentes de seguridad de la información. Para ello se debe: tener registro de eventos, registro del administrador y del operador y la sincronización de relojes.

5.1.21. Política de gestión de seguridad de las redes.

El objetivo es establecer los controles necesarios para proteger la información del Fondo transportada desde la red interna. La Oficina encargada de esta labor, es la responsable de administrar y gestionar la red del Fondo.

El trabajo a través de medios remotos a la red de datos del Fondo, sólo se permitirá de acuerdo a la Política de Teletrabajo establecida como tal. Es por ello que se debe: Contar con Separación de las redes.

5.1.22. Política de seguridad de la información para las relaciones con los proveedores.

El objetivo, establecer los criterios de seguridad la información para los datos accedidos por los proveedores. Se debe contar con: Consideraciones de seguridad en los acuerdos con terceras partes.

5.1.23. Política de gestión de incidentes de seguridad de la información.

El objetivo, gestionar adecuadamente, todos los incidentes de seguridad de la información reportados en El fondo, dando cumplimiento a procedimientos establecidos. Para ello debemos: Reportar los eventos y las debilidades de la seguridad de la información.

5.1.24. Política de gestión de la continuidad del negocio.

Objetivo es, garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información del Fondo. El fondo debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.

5.1.25. Política de gestión documental.

Esta política se definió e incorporó en el Pla de Privacidad y seguridad de la información del Fondo, para lo cual se tuvieron en cuenta las directrices definidas en el Decreto 2609 de 2012, Artículo 6, en el cual se establecen los componentes mínimos que debe incorporar. Esto lo aprobó El Comité Institucional de Desarrollo Administrativo.

5.2. Situación actual de la gestión de seguridad de la información-SGSI.

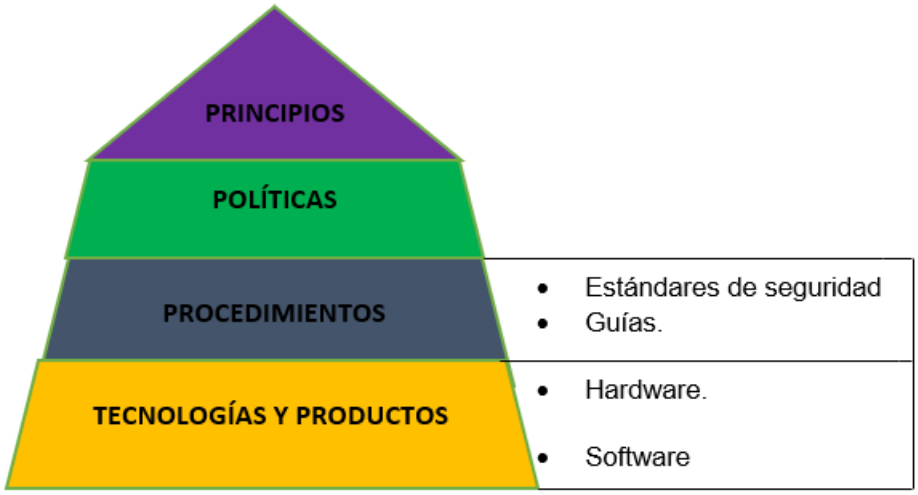
Actualmente y de acuerdo con la expedición del Decreto 2573 de 2014, contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones; El Fondo trabaja permanentemente en pos de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

En efecto, el modelo del SGSI del Fondo, se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que él esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

A continuación, se detallan cada uno de los componentes de fases del ciclo:

5.2.1. Descripción del modelo de seguridad de la información Actual.

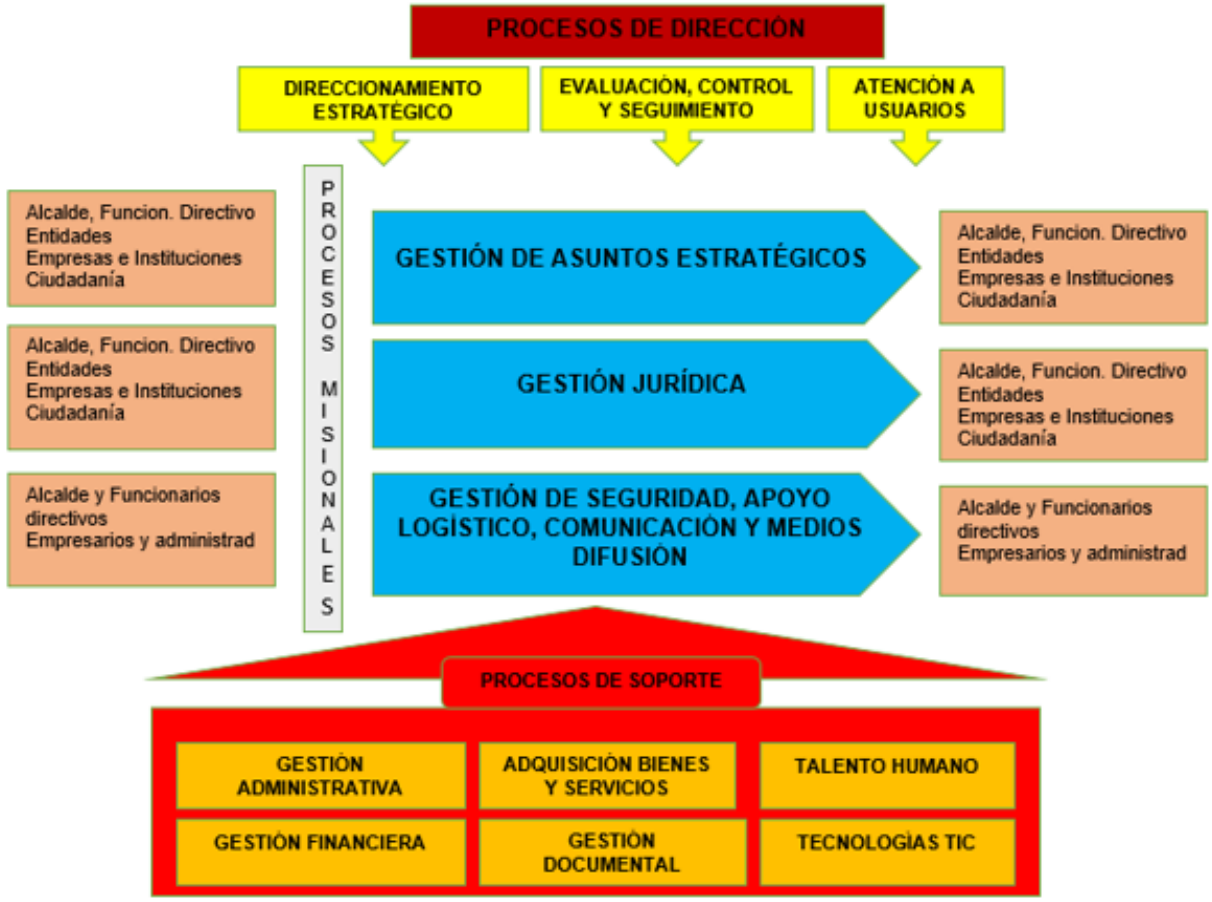
En el ámbito de la Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo a su importancia, a continuación, se ilustran dichos componentes:



Teniendo en cuenta el contexto interno y externo del Fondo, los grupos de interés en ambas dimensiones, e igualmente el alcance de SGSI, en términos de las características del Organismo, su ubicación, sus activos y su tecnología, definidos en los términos que se decidió, así:

“El Fondo Municipal de Tránsito y Transportes de Magangué, adopta, establece, implementa, opera, verifica y mejora el SGSI para los procesos misionales (3) y los procesos de apoyo (6) que componen el mapa de procesos de la entidad”; acorde con su naturaleza jurídica, misión y visión, encontró aplicables todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo A, sin excepción alguna.

En la siguiente ilustración, se muestran los procesos, aquellos que hacen parte del alcance del SGSI, éstos son los que están configurados en las áreas rojas.



5.2.2. Conceptos que apoyan la gestión de seguridad de la información-SGSI.

Para El Fondo, son muy importantes los resultados obtenidos en el Plan de Seguridad y Privacidad de la Información con el fin de apoyar la implementación del SGSI. El plan se apoya en el Plan Estratégico Institucional el cual a su vez se fundamenta en la metodología del Balanced Scorecard o Cuadro de Mando Integral, debido a su gran utilidad en el direccionamiento de las organizaciones.

El Balance Scorecard es una herramienta útil en la Planeación Estratégica. Esta metodología tiene en cuenta las siguientes fases: el análisis y revisión de la Misión, objetivos y estrategias, análisis de la propuesta de valor, recursos financieros, clientes, procesos, crecimiento y aprendizaje; reporte, revisión y comunicación de resultados, cambio y mejoramiento de las estrategias laborales de cada miembro de la entidad, actualización y adaptación permanente frente a cambios internos y externos del entorno. Asimismo, los objetivos y metas son evaluables y medibles, generando sus propios indicadores, que deberán ser utilizados como herramienta para el seguimiento, control, evaluación y gestión del Fondo.

En cuanto al contexto, en este punto del Plan de Seguridad y Privacidad de la Información, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están: La misión, La visión, Historia y antecedentes, Estructura organizacional, Procesos, Cultura y valores, Legislación pertinente y vigente.

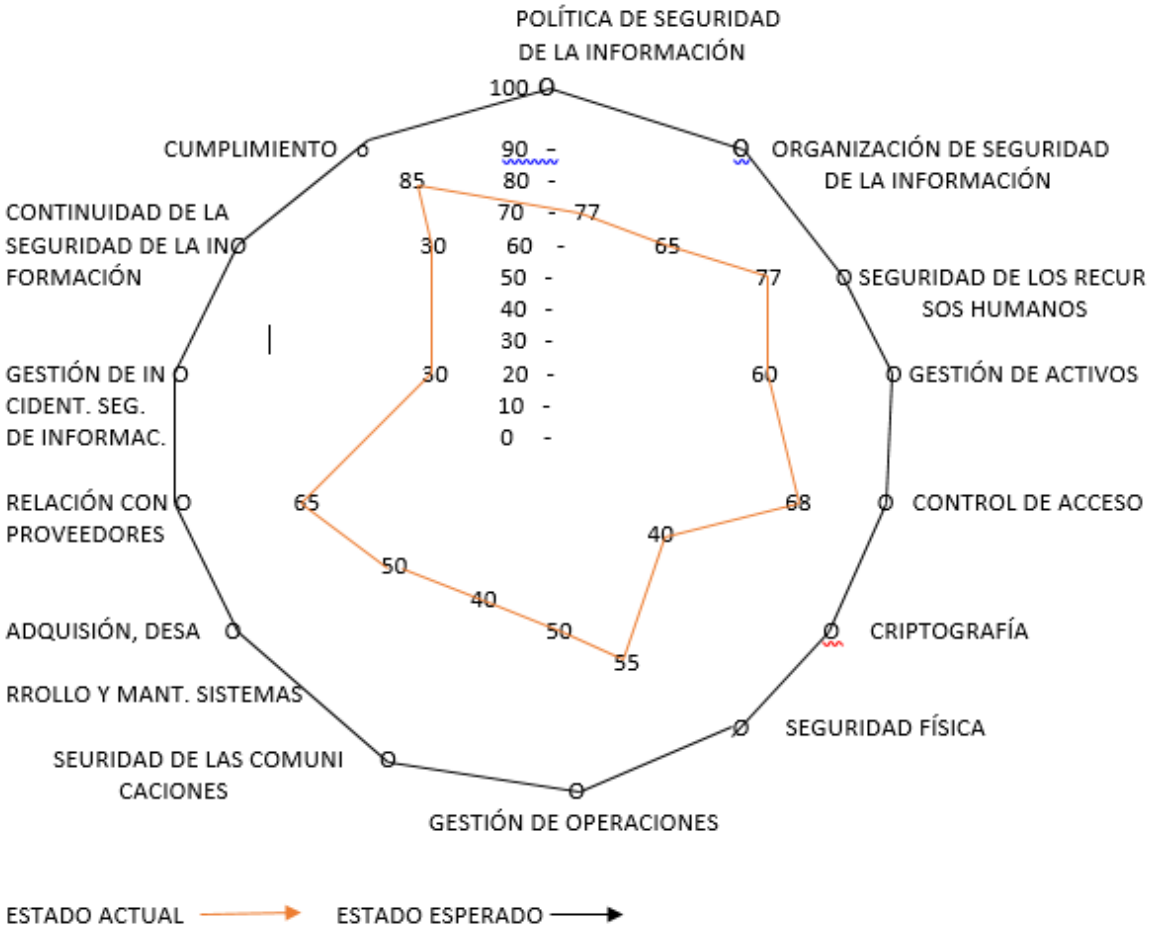
5.2.3. Estimación y Caracterización de la Situación Actual.

Para concretar la situación actual del Organismo, debemos conocer el nivel de madurez que posee en este momento El fondo, con relación a la seguridad de la información. El proceso por el cual se conoce esta estimación del nivel de madurez se denomina análisis GAP o análisis de brecha. Para poder realizar el Plan de Seguridad y Privacidad de la Información es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios (ver figura que se expone a continuación), con el fin de plantear prioridades sobre su implementación.

DOMINIO ISO 27001	OBJETIVO DEL CONTROL
Política de seguridad.	Objetivo de control 5.1. – 5.1.12.
Organización de La Seguridad de la información.	Objetivo de Control 5.1.11.
Seguridad de los RRHH.	Objetivo de Control 5.1.3.
Gestión de Activos.	Objetivo de control 5.1.21.
Control de Accesos.	Objetivo de Control 5.1.13.
Criptografía.	Objetivo de control 5.1.13.-5.1.10.
Seguridad Física y Ambiental	Objetivo de control 5.1.14
Seguridad en las Operaciones.	Objetivo de control 5.1.18. – 5.1.19. – 5.1.20.
Seguridad en las Comunicaciones.	Objetivo de control 5.1.4.- 5.1.5.- 5.1.6.- 5.1.7.- 5.1.8.
Adquisición de Sistemas, Desarrollo y Mantenimiento.	Objetivo de control 5.1.16.- 5.1.17.
Relación con Proveedores.	Objetivo de control 5.1.22.
Gestión de los Incidentes de Seguridad.	Objetivo de control 5.1.23.
Continuidad del Negocio.	Objetivo de control 5.1.24.
Cumplimiento de Requerimientos Legales y Contractuales.	Objetivo de control 5.1.9.- 5.1.25.

Para la aplicación de la metodología GAP, se hace el siguiente esquema de acciones:

En atención del ejercicio aplicativo GAP, se pudo constatar el nivel de avance de los elementos e instrumentos del SGSI del Organismo, el cual sintetizamos en la siguiente ilustración:



Analizando el gráfico anterior se puede concluir que los dominios que se encuentran en el nivel definido son: políticas de seguridad de la información, criptografía, seguridad física, gestión de operaciones y relaciones con los proveedores.

Los demás dominios se encuentran en los niveles: administrado, repetible y optimizado. En seguida, se presenta el grado actual de implementación y cumplimiento de la Entidad frente a los 14 dominios.

NUMERAL	CONCEPTOS DE DOMINIO	ESTADO ACTUAL	BRECHA	ESTADO ESPERADO	NIVEL
5.1.-5.1.12.	Política de Seguridad	77	23	100	Definido
5.1.11.	Organización Seguridad de la Información	65	35	100	Administrado
5.1.3.	Seguridad de los Recursos Humanos	77	23	100	Administrado
5.1.21.	Gestión de Activos	60	40	100	Administrado
5.1.13.	Control de Acceso	68	32	100	Administrado
5.1.10.-5.1.13.	Criptografía	40	60	100	Definido
5.1.14.	Seguridad Física	55	45	100	Definido
5.1.18. – 5.1.19. – 5.1.20.	Seguridad de Operaciones	50	50	100	Definido
5.1.4.- 5.1.5.- 5.1.6.-5.1.7.- 5.1.8.	Seguridad de las Comunicaciones	40	60	100	Repetible
5.1.16.-5.1.17.	Adquisición, Desarrollo y Mantenimiento de Sistemas	50	50	100	Definido
5.1.22.	Relación con Proveedores	65	35	100	Administrado
5.1.23.	Gestión de Incidentes de Seguridad de la Información.	30	70	100	Repetible
5.1.24.	Continuidad de Seguridad de la Información	30	70	100	Repetible
5.1.9.-5.1.24.	Cumplimiento	85	15	100	Definido
	PROMEDIO	**56,57**			**Definido**

5.2.4. Definición de Variables y Análisis de Posibilidades de Implementación.

Para la realización del análisis dentro del Plan de Seguridad y Privacidad de la Información es necesario definir una serie de variables que ayuden a priorizar los diferentes dominios de la NTC/ISO 27001-2013. Los 14 dominios de la norma están conformados por varios controles.

El Plan de Seguridad y Privacidad de la Información propone estrategias para la implementación basadas en una serie de variables que, permiten deducir el orden de implementación de cada uno de los dominios, teniendo en cuenta algunos aspectos asociados a cada uno de los controles. En la siguiente figura se presentan la matriz de valoración para cada una de las combinaciones posibles.

PRIORIZAR PLANEACIÓN	DOCUMENTACIÓN POLÍTICAS	DOCUMENTACIÓN PROCEDIMIENTOS	DOCUMENTACIÓN ESTÁNDARES
COSTO IMPLEMENTACIÓN	COSTO MANTENIMIENT	IMPLICACIONES	TIEMPO

Prioridad de la Planeación en el SGSI: Aquí se consideran los aspectos relacionados con el dominio desde el punto de vista de las categorías del tipo de control o dominio: administrativo, tecnológico y físico y los aspectos referentes a los niveles de planeación: estratégico, táctico y operativo. Combinación estos dos criterios (nivel de planeación y categorías del tipo del control o dominio), se les asigna un valor que ayudará a definir la prioridad de implementación teniendo en cuenta la magnitud de este valor tal como se muestra en la siguiente figura (los valores de mayor a menor son: 9, 6, 4, 3, 2,1).

CATEGORIAS				
	ESTRATÉGICO (3)	3	6	9
	TÁCTICO (2)	2	4	6
	OPERATIVO (1)	1	2	3
		FÍSICO (1)	TECNOLÓGICO (2)	ADMINISTRATIVO (3)
NIVELES DE PLANEACIÓN				

Estructuración y Documentación de la Política: El esfuerzo asociado con la documentación de políticas por cada uno de los dominios se mide en esta variable. La cantidad de políticas y normas que hay que desarrollar por dominio es un estimativo que ayuda a estimar su prioridad de implementación.

Los niveles utilizados para calificar este aspecto, se muestran a continuación:

Estructuración y Documentación de la Política		
VALOR	**NIVEL**	**RANGO # DE POLÍTICAS**
5	Muy Alto	Entre 10 y 11
4	Alto	Entre 7 y 9
3	Medio	Entre 5 y 6
2	Bajo	Entre 3 y 4
1	Muy Bajo	Entre 1 y 2

Documentación Procedimientos: El esfuerzo requerido por cada dominio en el número de procedimientos requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados, con el fin de asignarle una prioridad a la implementación de los diferentes dominios. Los valores estimados de criticidad relacionados con el número de procedimientos estimado requerido se presenta a continuación:

Documentación de Procedimientos		
VALOR	**NIVEL**	**RANGO # DE POLÍTICAS**
5	Muy Alto	Entre 8 y 9
4	Alto	Entre 6 y 7
3	Medio	Entre 4 y 5
2	Bajo	Entre 2 y 3
1	Muy Bajo	Igual a 1

Documentación estándares: El esfuerzo requerido por cada dominio en el número de estándares requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los dominios. Los valores estimados de criticidad relacionados con el número de estándares estimado requerido se presenta a continuación:

Documentación de Estándares		
VALOR	**NIVEL**	**CANTIDAD DE CRITERIOS**
5	Muy Alto	3
4	Alto	2
3	Medio	1
2	Bajo	0
1	Muy Bajo	0

Costo de implementación: Cada uno de los dominios de la norma dependiendo de la cantidad de herramientas, software, servicios, infraestructura, horas hombre, entre otros aspectos, requerirá de unos esfuerzos financieros diferentes. De tal manera que se puede recomendar como parte de este Plan, que aquellos dominios con menor costo sean implementados en el menor tiempo posible con el fin de obtener lo que se conoce como ganancias tempranas, lo que a larga beneficiará la aceptación de todo lo concerniente a la seguridad de la información por parte de la entidad y mantendrá la motivación en niveles altos, durante la fase de implementación del SGSI. La tabla utilizada para estimar de manera cualitativa el costo asociado a un dominio es la siguiente:

Costo de Implementación		
VALOR	**NIVEL**	**CRITERIOS (Miles de Pesos-$)**
5	Muy Alto	Mayor a 400.000
4	Alto	Entre 399.999 y 200.000
3	Medio	Entre 199.999 y 100.000
2	Bajo	Entre 99.999 y 50.000
1	Muy Bajo	Menor a 50.000

Gasto de Mantenimiento: Todo control asociado a un dominio tiene por su misma naturaleza unos gastos asociados en mantener su efectividad en el transcurso del tiempo. Estos gastos normalmente tienden a ser reiterativos y en algunos casos se requiere de un tercero para que cumpla con la función del mantenimiento. La tabla utilizada para estimar de manera cualitativa los gastos asociados a un dominio es la siguiente:

Gasto de Mantenimiento		
VALOR	**NIVEL**	**CRITERIOS (Miles de Pesos-$)**
5	Muy Alto	Mayor a 250.000
4	Alto	Entre 249.999 y 150.000
3	Medio	Entre 149.999 y 100.000
2	Bajo	Entre 99.999 y 50.000
1	Muy Bajo	Menor a 50.000

Complejidad: La variable complejidad considera las calificaciones requeridas en el recurso humano con el fin de acometer la implementación del dominio o control en cuestión, para ello se consideran los siguientes aspectos:

a) Especialista

b) Ingeniero

c) Técnico

d) Estudiante técnico o profesional

e) Personal no calificado

La tabla utilizada para estimar de manera cualitativa la complejidad asociada a un dominio es la siguiente:

Implicaciones		
VALOR	**NIVEL**	**CRITERIOS**
5	Muy Alto	Especialista
4	Alto	Ingeniero
3	Medio	Técnico
2	Bajo	Estudiante Técnico o Profes.
1	Muy Bajo	Personal no Calificado

• **Tiempo:** La variable tiempo le imprime al dominio unas restricciones importantes en lo referente al tema de cuándo se debe abordar su implementación. Se considera que si un control o dominio toma mucho tiempo para su implementación es recomendable abordarlo posteriormente para que de esta manera podamos implementar muchos más controles que sean de corta duración en su implementación y se aumenta rápidamente el porcentaje de cumplimiento de la norma de seguridad. No obstante, se debe considerar que estos controles de largo tiempo de implementación sean acometidos sin violar los requerimientos de tiempo de todo el proyecto.

La tabla utilizada para estimar de manera cualitativa el tiempo asociado a la implementación de un dominio determinado es la siguiente:

Tiempo		
VALOR	**NIVEL**	**CRITERIOS**
5	Muy Alto	Más de 1 Año
4	Alto	De 9 a 12 Meses
3	Medio	De 6 a 9 Meses
2	Bajo	De 3 a 6 Meses
1	Muy Bajo	Menos de 3 Meses

5.2.5. Presentación y Valoración de Resultados.

Con el fin de estimar las prioridades para cada uno de los dominios de la norma ISO 27001 se definieron una serie de variables que una vez calificadas se utilizaron para determinar la prioridad estratégica de implementación de los dominios y que fueron presentadas anteriormente. A continuación, se presenta la tabla con las variables que permiten estimar la Prioridad Estratégica de cada uno de los dominios de la norma. Esta Prioridad se estima en porcentaje lo que nos permitirá luego ordenar cada uno de los dominios y definir las 3 fases de implementación:

VARIABLES PARA EL ANÁLISIS								
Prioridad en Planeación	Esfuerzo Documental			Calificación de la Implementación				Prioridad Estratégica (%)
	Políticas	Procedim.	Estándar.	Costo Implementac.	Costo Manten.	Implicac.	Tiempo	
5	1	1	1	1	1	4	3	25,00 %

Con base en la prioridad estratégica procedemos a definir las diferentes fases que conformarán el proceso de implementación de los dominios de la norma. Se determinaron tres (3) fases principales para la implementación de todos los dominios. El tiempo estimado aproximado para la finalización de estas fases es de tres años, teniendo en cuenta aspectos legales, contractuales y la experiencia nuestra por la situación del Organismo, obviamente contando con la dedicación del líder de seguridad y los analistas sugeridos en el Manual del SGSI. También a todo lo anteriormente expresado subyace la premisa de implementar los controles que toman menos tiempo y requieren menor esfuerzo, según lo reflejado por las variables definidas para el análisis del Plan de Seguridad y Privacidad de la Información.

DOMINIO	PRIORIDAD EN %	ETAPAS
5.1.-5.1.12. Políticas de Seguridad de la Información.	100%	1
5.1.11. Organización de Seguridad de la Información	5%	3
5.1.3. Seguridad de los Recursos Humanos	12%	2
5.1.21. Gestión de Activos	10%	2
5.1.13. Control de Acceso	6%	3
5.1.10.-5.1.13. Criptografía	30%	1
5.1.14. Seguridad Física.	3%	3
5.1.18. –5.1.19.–5.1.20. Seguridad de las Operaciones	10%	2
5.1.4.- 5.1.5.- 5.1.6.-5.1.7.- 5.1.8. Seg. Comunicaciones	8%	3

5.1.16.-5.1.17. Adquisición, Desarr. y Manten. Sistema	5%	3
5.1.22. Relación con Proveedores.	15%	2
5.1.23. Gestión Incidentes de Seg. de la Información	20%	1
5.1.24. Continuidad Seguridad de la Información	8%	3
5.1.9.-5.1.24. Cumplimiento	30%	1

En la siguiente gráfica se pueden observar los dominios asociados por cada una de las fases consideradas, teniendo en cuenta la prioridad estratégica calculada para los dominios. Los dominios de la Fase I, II y III están señalados según los colores del semáforo.

5.3. Pasos y Secuencias Para Implementación.

5.3.1. Políticas de Seguridad de la Información.

La política determina los objetivos de seguridad, lo que se quiere hacer en temas de seguridad, se basa en los análisis de riesgos y en los resultados de la gestión de incidentes de seguridad. Las políticas siempre responden a la pregunta ¿Qué voy a hacer? y en ese sentido hay que redactar la política. La política define los objetivos a alcanzar y no cómo se va a implementar, es un error incluir en una política algo operativo por ej. “la contraseña debe tener 8 caracteres alfanuméricos, al menos una mayúscula y números”, esto no es una política, sino la forma como cumpliría el objetivo, responde a cómo lo voy a hacer y no a ¿qué voy a hacer? una política correcta podría ser algo como “Todos los usuarios que acceden a los sistemas de información del Organismo, deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal.”. Lo anterior, lo que se refería a las características de las contraseñas, es lo que se conoce como norma, la cual, no es otra cosa, que enunciados de obligatorio cumplimiento, que responden a la forma en que se cumplirá una política.

Como se mencionó anteriormente, la política determina los objetivos de seguridad, y la forma de cumplir con estos objetivos en el modelo de seguridad es a través de normas y procedimientos. Las normas y procedimientos siempre deben responder a una política, por lo tanto, en cada norma o procedimiento debe especificarse a qué política responde, si no se puede determinar a qué política corresponde debe razonarse, o que el procedimiento o norma no es necesario, o que el documento de políticas está incompleto. El documento de políticas SIEMPRE debe ser conocido y firmado por la alta dirección.

Como ayuda para elaborar el documento de políticas del Organismo, se debe revisar la norma GTC/ISO 27002:2015 y adicionalmente adquirir en la medida de lo posible plantillas para la implementación de políticas que se pueden conseguir en internet. Las políticas se deben revisar periódicamente, y medir la eficiencia y eficacia con la que se están cumpliendo estos objetivos de seguridad, por lo que El

Organismo debe implementar un procedimiento del área de seguridad de la información que estandarice el mecanismo por el cual se realizan las revisiones periódicas de los documentos del modelo de seguridad (incluyendo el documento de políticas), de manera que forme parte del modelo de seguridad y sea sujeto de ser auditado.

5.3.2. Organización de la seguridad de la Información.

La seguridad de la información realmente es una cultura, en la cual se deben involucrar todos los colaboradores, tanto servidores públicos, usuarios y contratistas para que contribuyan a crear un clima de seguridad tanto al interior como al exterior de la entidad. La organización de seguridad debe estar distribuida por toda la entidad en diferentes funciones con responsabilidades relacionadas con la seguridad de la información. Se deben utilizar roles para la realización de las actividades que los colaboradores realizan en cada procedimiento, y posteriormente asociar a los cargos, los roles previamente definidos, que contienen las actividades y las funciones de cada rol. A la hora de realizar esta asignación de roles a cargos se debe:

1. Realizar una matriz RACI2 para cada procedimiento, de tal forma que puedan ser controladas las actividades por diferentes personas.

2. Realizar una matriz de segregación de funciones entre los roles con el fin de asegurarse que para un cargo no se presenten conflictos de intereses en temas de seguridad de la información. Dentro del modelo de seguridad, la organización de seguridad debe tener al menos:

- Un comité de seguridad de la información en el cual se debe integrar la alta gerencia. Este comité es el órgano máximo del modelo de seguridad. Sus funciones principales, entre otras, podrían ser:

o Definir los lineamientos y estrategias de Seguridad de la información en función de los objetivos del negocio.

o Aprobar el modelo de seguridad de la entidad (políticas, normas, procedimientos, etc.).

o Aprobar el Plan de seguridad y Privacidad de la Información, así como los resultados de su implementación.

- Líder de seguridad de la Información de la Entidad. Es el encargado de coordinar todo el modelo de seguridad. Debería estar dedicado tiempo completo a temas de seguridad y debe velar por el mejoramiento continuo del modelo de seguridad. Debe establecer contacto con las autoridades pertinentes, así como con grupos de interés en temas de seguridad.

- Analista de se seguridad de la información. Son funcionarios dedicados tiempo completo a temas de seguridad de la información y que realizan labores operativas

del modelo de seguridad. Son dirigidos por el líder de seguridad de la información. En lo posible, la entidad debe contar como mínimo con dos funcionarios para este rol. Otros roles sugeridos a futuro dentro de la entidad de seguridad podrían ser: • Administrador de recursos informáticos.

• Administrador de control de acceso lógico.

• Operador de seguridad de la información.

• Líder de seguridad física.

• Líder de recursos humanos

• Líder de organización y métodos o líder del sistema de calidad.

• Auditor de Seguridad.

• Asesor legal Entre otros… Este dominio también contempla el aseguramiento de dispositivos móviles y el teletrabajo. Con referencia a este tema se sugieren las siguientes recomendaciones:

• Contar con un inventario con el registro de todos los dispositivos móviles de la entidad, en el cual se registre al menos: la persona responsable del dispositivo, los activos de información que maneja el dispositivo y los lugares a los que tiene acceso.

• Contar con estándares de seguridad para dispositivos móviles que pueden contener entre otras, cifrado de disco duro, restricciones de instalación de software, actualización de parches de seguridad, restricción a conexiones de acceso de información, protecciones contra software malicioso, deshabilitar borrado remoto, copias de respaldo, entre otros.

• Contar con un documento formal de normas para uso de dispositivos móviles, donde se den recomendaciones sobre el uso de los dispositivos móviles y los cuidados de seguridad que se deben tener.

5.3.3. Seguridad del Recurso Humano.

Con relación a la seguridad de los recursos humanos se debe tener en cuenta el ciclo de vida del recurso humano, esto es, antes, durante y después de su contratación. En este sentido se darán recomendaciones en estas tres etapas. Antes de la contratación: Contar con un procedimiento de selección de personal que, de acuerdo con las leyes y reglamentos de ética pertinentes, incluya:

• Verificación de referencias.

• Verificación de la hoja de vida completa.

• Verificación de la identidad del aspirante.

- Verificación de competencia.
- Pruebas psicotécnicas.
- Verificar en términos generales que sea una persona confiable.

Durante el periodo de contratación:

- Todos los colaboradores y contratistas que accedan a información reservada o sensible deben firmar un acuerdo de confidencialidad y no divulgación ANTES de tener acceso a dicha información por cualquier medio.
- Todos los colaboradores deben firmar una cesión de derechos de propiedad intelectual a favor de la entidad sobre los desarrollos que se realicen fruto de su trabajo en la entidad.
- Todos los colaboradores deben seguir fielmente las normas sobre el manejo de cada tipo de información de acuerdo con lo definido en la clasificación de activos de información.
- Contar con un proceso disciplinario sí se incumple cualquiera de las normas de seguridad establecidas.
- Contar con un proceso disciplinario frente a la responsabilidad en incidentes de seguridad de la información en los que se demuestre la participación de algún colaborador.
- Brindar capacitaciones del modelo de seguridad aprobado, así como capacitaciones periódicas en temas de seguridad con el fin de tomar conciencia sobre la seguridad de la información pertinente a sus roles, y lograr crear una cultura de seguridad al interior y exterior de la entidad.
- Contar con un canal anónimo mediante el cual los colaboradores puedan reportar posibles incidentes de seguridad de la información. Se debe crear un programa de capacitaciones continuas en seguridad que deberán cubrir como mínimo los siguientes aspectos:
- Concientización sobre riesgos de seguridad.
- Conocimiento del modelo de seguridad.
- Conocimiento de las normas y procedimientos de seguridad.
- Puntos de contacto para información de problemas de seguridad.
- Mecanismos para el reporte de incidentes de seguridad de la información.
- Tips prácticos de seguridad orientado a las labores que realiza cada colaborador según sus funciones.

Al terminar la contratación:

• Dentro del procedimiento de terminación de contrato se debe incluir: backup de la información que el colaborador manejaba, eliminación de todos los usuarios y contraseñas del colaborador, eliminación de los accesos remotos de teletrabajo a los que tenía acceso el colaborador.

• El área de seguridad de la información debe dar un visto bueno, o un paz y salvo después de analizar que los activos de información permanezcan en la entidad. Este paz y salvo debe ser requisito para completar el proceso de desvinculación.

5.3.4. Gestión de Activos.

Este dominio pretende identificar los activos de información de la entidad, clasificarlos, asignarles responsables a dichos activos y brindarles un tratamiento apropiado de acuerdo a su clasificación. Las recomendaciones en este punto son:

• Realizar un inventario de todos los activos de información, para este fin normalmente se realiza una búsqueda de los activos de información en los procesos y procedimientos, buscando el flujo de información en los mismos.

• Incluir en el inventario, el tipo de activo (físico o digital), ubicación, activos de soporte, redes, medios, servidores o servicios en las que se encuentra, proceso al que pertenece, entre otros.

• Asignar a cada activo de información un dueño. El dueño del activo de información es el responsable del activo de información y velará por salvaguardar dicho activo y hacer cumplir el tratamiento de seguridad del mismo de acuerdo con su clasificación. Se considera a los activos de información como cualquier otro activo, con un valor financiero y estratégico.

• Realizar una clasificación de los activos de información teniendo en cuenta criterios de disponibilidad, integridad y confidencialidad de dicha información.

• Asignar un tratamiento de seguridad detallado para cada nivel de la clasificación de los activos de información, definiendo normas de uso, etiquetado, y controles de seguridad para cada nivel de clasificación. Cuando se terminen los vínculos contractuales con la entidad se debe devolver todos los activos de información a los que el colaborador tuvo acceso.

Con respecto a la gestión de medios removibles, se debe:

• Inicialmente bloquear todos los accesos a medios removibles en todos los equipos de la entidad (bloqueo de USB).

• Habilitar los puertos USB, sólo con una justificación escrita y debe ser autorizada por el área de seguridad. Sólo se deberá habilitar el uso de medios removibles, si hay una razón de negocio para hacerlo.

- Se deben redactar normas para el uso de dispositivos removibles.

- Se debe tener registro de la información en medios removibles.

- Sí la información ya no se requiere tener en dispositivos removibles o cuando el colaborador se retire de la entidad, debe realizarse un borrado seguro del medio removible.

- Sí la confidencialidad o integridad de la información contenida en un medio removible se considera importante, debería utilizar mecanismos criptográficos apropiados para cada medio.

- La disposición final para los medios removibles debe realizarse en forma segura, por ejemplo, incineración o borrado seguro.

5.3.5. Control de Acceso.

El objetivo del dominio de control de acceso consiste en limitar el acceso a la información y a las instalaciones con el fin de salvaguardar los activos de información.

- Se debe realizar unas políticas de control de acceso, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones para esta política son:

o Tener en cuenta para este fin la clasificación de la información, la legislación pertinente de acuerdo con las leyes de protección de datos.

o Implementar un procedimiento de gestión de derechos de acceso a los diferentes tipos de activos de información en los que se involucre a los dueños de los activos de información.

o El criterio fundamental a la hora de definir la política de control de acceso debería ser: “Permitir sólo lo que necesita conocer para realizar sus funciones, de lo contrario no se permite”

- Se debe realizar unas políticas de control de acceso a redes y servicios de red, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones al respecto son:

o El acceso a redes o servicios de red debe justificarse en función de los activos a los que se necesita acceder, en la clasificación de los activos puede encontrar en qué redes o a que servicios se le debe permitir acceso para acceder al activo de información.

o Se debe incluir procedimientos para monitorear las redes, tráfico y quién tiene acceso de acuerdo con la política, y en caso de accesos no autorizados, considerarlos como un incidente de seguridad e iniciar inmediatamente una investigación de seguridad.

- Se debe implementar un procedimiento de gestión de acceso a usuarios. Este procedimiento incluye la creación, modificación y eliminación de usuarios. Generalmente está asociado con el proceso de contratación y desvinculación. El procedimiento debe tener en cuenta la autorización al acceso de activos de información, redes y servicios, y estas autorizaciones deben ser avaladas por el dueño del activo de información y por el área de seguridad de la información como mínimo.

- Se debe revisar periódicamente todos los accesos a los activos de información, redes y servicios. En estas revisiones identificar y eliminar o deshabilitar permisos redundantes y obsoletos de acuerdo con las solicitudes de acceso.

- Se debe tener especial cuidado con usuarios con altos privilegios.

- Se debe habilitar logs de acceso a los sitios restringidos.

- Se debe realizar auditoría periódica a los permisos de acceso.

- A nivel de aplicativos, durante su desarrollo, desde la etapa de diseño, se debe tener en cuenta:

o La posibilidad de restringir el acceso a la información de la aplicación, para esto utilizar roles, permitir auditar el acceso a información sensible y a operaciones sensibles dentro del aplicativo, entre otras.

o Utilizar técnicas de autenticación adecuadas para corroborar la identidad de un usuario.

o Durante el log-on se debe proteger de intentos de ingreso por fuerza bruta, evitar mensajes de ayuda en el log-on, utilizar contraseña protegida (que no se vea la contraseña al momento de ingresarla), llevar registro de intentos de log-on (exitosos y fallidos). No transmitir las contraseñas en texto plano.

o Se debe cerrar las sesiones por inactividad.

5.3.6. Criptografía.

El objetivo de este dominio es asegurar la confidencialidad mediante el uso de métodos apropiados de criptografía. Los sistemas centralizados de gestión de llaves garantizan la seguridad de las diferentes llaves utilizadas por los sistemas de cifrado. Los proyectos recomendados para este dominio son:

5.3.7. Seguridad Física y del Entorno.

La seguridad no es una tecnología, ni un producto, es un proceso que se apoya en la tecnología para lograr sus objetivos a lo largo de toda la entidad. La seguridad debe ser un enfoque sistémico realizado por profesionales en la materia, que propongan una serie de actividades, procesos y productos para que todos funcionando de manera sincronizada ejerzan un control, factores disuasivos, e

información; que en su conjunto garanticen que la entidad pueda lograr sus objetivos de manera oportuna y productiva.

La seguridad física en Colombia es y ha sido un aspecto muy importante de la forma como las empresas protegen sus activos económicos. Se requiere contar con una metodología que permite evaluar qué tan efectivos son los controles existentes en la infraestructura de la Entidad con el fin de actuar como factor disuasivo y control, contra eventos que pongan en peligro la disponibilidad, confidencialidad e integridad de la información.

Es importante considerar que factores como el control de variables ambientales, tecnologías de control de acceso, y sistemas de CCTV, permiten implementar los controles. Estos controles deben ser el resultado del análisis de riesgo, en donde se determinan las prioridades de cada uno de los elementos anteriormente mencionados.

Zonas de mejora o posibles proyectos (mejora de controles de acceso y protección contra amenazas naturales)

1. Centros de Procesamiento normales o de emergencia.

2. Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación.

3. Áreas donde se encuentren concentrados dispositivos de información.

4. Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos.

5. Duros, Cintas etc.).

6. Áreas donde se deposite salidas de impresoras o fax. Normas que se deben aplicar en El Organismo.

• Código Eléctrico Colombiano, NTC 2050, 1986.

• Acuerdo 20 del Distrito, Código de Construcción.

• NFPA 70 National Electrical Code (NEC), 2005.

• ANSI/TIA 942, Telecommunications Infrastructure for Data Centers Standard.

• Manual de Métodos de Distribución de Telecomunicaciones (TDMM) de Bicsi. Capítulo 8, “Equipment Room”

• NFPA 75 Standard for the Protection of Electronic Computer/Data Processing Equipment, 2.003 Edition.

• IEEE 1100-2005, Recommended Practice for Powering and Grounding Sensitive Electronic Equipment.

• TIA/EIA 568 B2.1 Commercial Building Telecommunications Wiring Standards.

• TIA/EIA 569A Commercial Building Standard for Telecommunications Pathways and Spaces.

• Thermal Guide for Data Processing Environments. ASHRAE (American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc).

• Recomendaciones de fabricantes de equipos de cómputo para instalación de sus equipos (site prep).

5.3.8. Seguridad en las Operaciones.

El objetivo de este dominio consiste en asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. Para ello, lo divide en siete grandes subdominios que se tratarán individualmente:

5.3.8.1. Procedimientos Operacionales y Responsabilidades.

Para este subdominio se debe:

• Tener procedimientos documentados de cada uno de los elementos de procesamiento de información, como servicios, aplicativos, dispositivos de red y de infraestructura. La documentación por cada elemento debería incluir como mínimo: o Instalación y configuración de los sistemas o Procedimientos de encendido y apagado o Procedimientos de respaldo tanto de los datos como de la configuración.

• Contar con un procedimiento de gestión de la capacidad. El principio fundamental consiste en monitorear todos los recursos de procesamiento y comunicación, tales como ancho de banda de los canales, memoria, capacidad de almacenamiento, capacidad de cálculo, entre otros, y alertar cuándo lleguen a valores críticos con el fin de gestionar la capacidad de cómputo, bien sea optimizando o adquiriendo más capacidad.

• Contar con separación de ambientes, la norma se refiere a que el ambiente de desarrollo debe ser diferente al ambiente de producción. Cuando se refiere a ambientes, lo ideal sería que fuesen ambientes totalmente independientes. En lo posible, se debe procurar cinco ambientes como se describen a continuación:

o Terceros: cuando se desarrolla software por terceros y es necesario que tengan acceso a los sistemas de la entidad, es recomendable construir un ambiente independiente para el proveedor que no interfiera con la entidad ni afecte la seguridad de la misma. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.

o Desarrollo: El ambiente de desarrollo es un ambiente diseñado para este fin no debe tener acceso directo a los sistemas de producción. Debería brindarle a los desarrolladores una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.

o Pruebas y Calidad de Software: Es un ambiente destinado para todas las pruebas de software: funcionales, no funcionales y pruebas de seguridad. Debería tener una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.

o Producción: Es el ambiente productivo, donde se realizan las operaciones reales de la entidad.

o Contingencia: Es el ambiente de respaldo que se analiza en detalle en la gestión de continuidad, debe ser lo suficientemente robusto para soportar los servicios mínimos requeridos por la entidad.

5.3.8.2. Registro y Seguimiento.

El objetivo de este subdominio es dejar rastro de los eventos y evidencia de todas las operaciones relevantes con el fin de que sirvan de apoyo en una investigación de seguridad en un momento dado. Se debe tener en cuenta para estos registros que contengan entre otros la siguiente información:

- Identificación de usuarios;
- Actividades del sistema;
- Fechas, horas y detalles de los eventos clave, por ejemplo, entrada y salida;
- Identidad del dispositivo o ubicación, si es posible, e identificador del sistema;
- Registros de intentos de acceso al sistema exitosos y rechazados;
- Registros de datos exitosos y rechazados y otros intentos de acceso a recursos;
- Cambios a la configuración del sistema;
- Uso de privilegios;
- Uso de utilidades y aplicaciones del sistema;
- Archivos a los que se tuvo acceso, y el tipo de acceso;
- Direcciones y protocolos de red;
- Alarmas accionadas por el sistema de control de acceso;
- Activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;
- Registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

5.3.9. Seguridad en las Comunicaciones.

La transferencia de información está expuesta a múltiples riesgos, por ello la entidad debe implementar medidas preventivas para evitar su divulgación o modificación. Para lograr esto la ESAP debe: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte y mantener la seguridad de la información transferida dentro de la entidad y con cualquier entidad externa.

5.3.10. Adquisición, Desarrollo y Mantenimiento de Sistemas.

La seguridad en los procesos de desarrollo de software debe estar a lo largo de cada parte del ciclo de desarrollo de software, las recomendaciones por cada parte son:

Análisis de Requerimientos

- Definir claramente con el usuario final el alcance de los requerimientos.
- Determinar la confidencialidad de la información que se maneja.
- Definir el control de autenticación requerido.
- Definir los roles y los privilegios de cada rol.

Diseño.

- Acceso a componentes y administración del sistema.
- Logs para auditoría.
- Datos históricos.
- Manejo apropiado de errores.
- Segregación de funciones.
- Defina adecuadamente la administración de identidades

o Exija el uso de contraseñas seguras.

o En el caso de que se produzca un error en la autenticación, devuelva la mínima información posible.

- Compruebe siempre la validez de los datos de entrada.

o Suponga que todos los datos especificados por los usuarios tienen mala intención.

o Compruebe la validez del tipo, longitud e intervalo de los datos.

- Administración de la configuración y las sesiones.
- Datos confidenciales y criptografía.

- Auditoría y registro, siempre dejar registro de las actividades sensibles del aplicativo, (login y log-out, Tiempo de sesión, accesos a la base de datos).

Codificación.

- Aseguramiento de los ambientes de desarrollo.
- Mantener documentación técnica.
- Seguridad en las interfaces de comunicación.
- Buenas prácticas de codificación:

o Validación de entradas.

o Codificación de las salidas.

o Estilo de programación limpio.

o Código autodocumentado o Control de código fuente (log de cambios) o Buena utilización de recursos (memoria, acceso a base de datos).

o Estandarización y reutilización de código.

Pruebas.

- Controles de calidad en controles de seguridad.
- Inspección de código por fases.
- Realizar pruebas de caja blanca y caja negra (owasp top 10) Instalación, actualización y parches.
- Tener en cuenta control de cambios.
- Comprobación de gestión de configuraciones

5.3.11. Relaciones con los Proveedores.

Los proveedores por su naturaleza son una de las fuentes externas de riesgos, pero a su vez son importantes para el cumplimiento de la misión y la visión de la entidad, por esta razón se deben implementar controles para: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores y mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con proveedores. Las auditorías nos ayudan a determinar el nivel de cumplimiento de los proveedores con respecto a la seguridad de la información:

5.3.12. Gestión de Incidentes de Seguridad de la Información.

Construir un proceso consistente para gestionar los incidentes de seguridad de la información, el cual debe contener como mínimo:

- Reporte de incidente de seguridad de la información.

- Investigación de incidente de seguridad de la información.

- Adecuado control de cadena de custodia para gestión de evidencias. La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

5.3.13. Seguridad de la Información de la Gestión de Continuidad de Negocio.

La continuidad del negocio en lo relacionado a la información es un componente fundamental en la implementación del SGSI. La Gestión de la Continuidad del Negocio (BCM, por sus siglas en inglés Business Continuity Management) debe ser un proceso establecido en nuestra sociedad moderna, globalizada, interconectada, con tecnologías novedosas, más complejas y, además, con una alta presencia de riesgos de tipo operativo que en cualquier momento podrían llegar a materializarse.

Finalmente, el BCP ha sido estandarizado en el año 2012 bajo la norma internacional ISO 22301; norma certificable que ha servido de consulta permanente e indispensable para la realización de este documento y del proceso en general.

Recientemente, se ha concedido una importancia creciente a la implementación de planes, procedimientos y estructuras que garanticen la continuidad de los productos y servicios críticos de una determinada organización ante incidentes de diversas categorías y de diferentes niveles de impacto.

Estos factores, junto con una legislación cada vez más exigente en lo relacionado a la confiabilidad y a la seguridad en la prestación de estos productos y servicios, hacen necesario, en la actualidad, que se cuente con un BCP/DRP con el objetivo de lograr una sociedad cada vez más comprometida con la protección del talento humano, con la disponibilidad de los procesos del negocio, con la protección de la información (ISO 27001:2013), con fortalecimiento y preservación del conocimiento, con la tecnología propicia y segura, al igual, que con el incremento de la productividad, la agilidad, la efectividad y la eficiencia.

En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, pero las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las pandemias, la pérdida de empleados claves, las amenazas naturales y el CIBERTERRORISMO3, entre otros, han mostrado la necesidad de incorporar nuevas amenazas en el BCP con el fin de garantizar la continuidad de las operaciones ante un escenario cada vez más dinámico en lo relacionado con el tipo de riesgos al que se está expuesto. De acuerdo con la firma Continuity Software de los Estados Unidos, las fallas a nivel de hardware en los diferentes dispositivos que conforman los sistemas de información,

por dos años consecutivos, han permanecido en el primer lugar, como causa de activación de los BCP, de acuerdo al 55% de los encuestados, le siguen migraciones de tecnología con el 51%; en el 2014, el error humano alcanzó un 47% y las fallas a nivel de las aplicaciones un 43%.

5.3.13.1. Proyectos o Planes Anexos a la Continuidad de Actividades.

5.4.113.1.1. Plan de Comunicación de Crisis.

Busca describir los procedimientos y comunicados que las organizaciones deben preparar para responder ante un incidente de manera correcta. Este plan debe estar coordinado con los otros planes de la organización para asegurar que sólo comunicados revisados y aprobados sean divulgados y que solamente el personal autorizado, previamente designado, sea el responsable de responder a las diferentes inquietudes y de diseminar los reportes de estado durante la contingencia a los empleados y al público en general.

5.3.13.1.1. Planes de Evacuación por Edificio.

Estos planes contienen los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y a la seguridad del personal, al ambiente o a la propiedad. Tales eventos podrían incluir fuego, terremoto, huracán, ataque criminal o una emergencia médica, entre otros. Estos planes son normalmente desarrollados a nivel de instalación, específicos a la localización geográfica y al diseño estructural de la construcción.

5.3.13.1.3. Plan de Respuesta a CIBERINCIDENTES.

Este plan establece los procedimientos Plan de respuesta a CIBERINCIDENTES: este plan establece los procedimientos para responder a los ataques en el ciberespacio contra los sistemas de información de una organización. Son diseñados para permitirle al personal de seguridad identificar, mitigar y recuperarse de incidentes de cómputo maliciosos tales como: acceso no autorizado a un sistema o información, negación del servicio, cambios no autorizados al hardware y al software, entre otros. Ejemplos de elementos que pueden generar estos incidentes de seguridad pueden ser: la lógica maliciosa, los virus, los gusanos, los troyanos, por mencionar algunos. Estos planes normalmente pueden pertenecer o estar integrados al Sistema de Gestión de la Seguridad de la Información (SGSI), normalmente estipulados y estandarizados bajo la norma ISO 27001:2013.

5.3.1.13.1.4. Plan de Recuperación de Desastres.

Este plan es conocido como DRP (Disaster Recovery Plan), y está orientado a responder a incidentes, usualmente catastróficos, que puedan afectar la prestación de los servicios de información. Frecuentemente, el DRP se refiere a un plan

enfocado en TI, diseñado para restaurar la operatividad de los sistemas, aplicaciones y bases de datos. Por otra parte, como parte del DRP, se cuenta generalmente con un sitio alterno en donde se realizarán las operaciones, definidas por el BIA, que fueron interrumpidas por el incidente o desastre en el sitio principal. El alcance de un DRP puede confundirse con el de un Plan de Contingencia de TI; sin embargo, el DRP es menos amplio en alcance y no cubre interrupciones menores que no requieran reubicación.

5.3.13.1.5. Planes de Contingencia.

Según el NIST (National Institute of Standards and Technologies), los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y a recuperar los servicios críticos de TI, después de una interrupción, en el menor tiempo posible. Es factible en algunos casos contar con múltiples planes de contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contingencia son de rápida activación y se puede asumir un RTO (Recovery Time Objective: Tiempo Objetivo de Recuperación), muy cercano a cero. Los planes de contingencia son típicos en los canales de comunicaciones y servidores, de tal manera que, ante la falla de uno de estos canales o servidor, otro, entrará en operación muy rápidamente y, en muchos casos, de manera automatizada.

5.14. Cumplimiento.

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o a las finanzas de la entidad.

Definir procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados, en el marco de la Ley 719 de 2001.

Establecer una política de privacidad y protección de la información de datos personales, en el marco de la Ley 1581 de 2012 y mantener una capacitación continua sobre estas leyes con expertos en el tema.

Adicionalmente, como parte del ciclo de mejoramiento continuo del SGSI, la entidad debe garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos organizacionales.

6. PROYECTOS A IMPLEMENTAR EN EL SGSI.

A continuación, se presenta una caracterización básica de las iniciativas en las fichas técnicas por cada uno de los proyectos a implementar:

6.1. Establecimiento de políticas de seguridad y privacidad de la información.

ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN			
OBJETIVOS DEL PROYECTO	Definir y establecer un conjunto de políticas para la seguridad y privacidad de la información, aprobada por la dirección, publicada y comunicada a las partes interesadas de la entidad.		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.-5.1.12. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN 5.1.11. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN 5.1.10.-5.1.13. CRIPTOGRAFÍA 5.1.114. SEGURIDAD FÍSICA Y DEL ENTORNO 5.1.18.-5.1.19.5.1.20. SEGURIDAD DE LAS OPERACIONES 5.1.22. RELACION CON LOS PROVEEDORES 5.1.9.-5.1.24. CUMPLIMIENTO		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Bajo (De 3 a 6 meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Bajo (Entre 99.999 y 50.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	PLANEACIÓN GESTIÓN TECNOLÓGICA GESTIÓN JURÍDICA Y ASUNTOS LEGALES LAS DEMÁS ÁREAS	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			
El alcance de la ejecución del proyecto incluye: *La definición y establecimiento de un conjunto de políticas para la seguridad y privacidad de la información, aprobada por la dirección, publicada y comunicada a las partes interesadas de la entidad.			
POTENCIALES BENEFICIOS ESPERADOS			
*Estas políticas le permitirán a la entidad garantizar la confidencialidad, la integridad y la disponibilidad de la información que los procesos necesitan para cumplir con la misión, la visión y los requerimientos estipulados en el Modelo de Seguridad y Privacidad de la Información - MSPI.			
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS			
*Porcentaje de ejecución del cronograma del proyecto			
PROYECTOS RELACIONADOS			
P2 - INTEGRACIÓN DEL PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON EL PIC P3 - AFINAMIENTO DE DATACENTER P6 - PRUEBAS ETHICAL HACKING P7 - IMPLEMENTACIÓN MODULO SGSI EN LA HERRAMIENTA ISOLUCIÓN			
COMPONENTE DE GOBIERNO EN LÍNEA			
*Seguridad y Privacidad de la Información			
ALINEAMIENTO ESTRATÉGICO SECTORIAL			
*PETI			
FACTORES CRÍTICOS DE ÉXITO			
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva			
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo		
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información		

6.2. Integración del Plan de Sensibilización y Capacitación de Seguridad y Privacidad de la Información con el Pic.

INTEGRACIÓN DEL PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN CON EL PIC

OBJETIVOS DEL PROYECTO	Integrar el Plan de Sensibilización y Capacitación de seguridad y Privacidad de la información con el Plan Institucional de Capacitación - PIC vigente en El Organismo.		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.3. SEGURIDAD DE LOS RECURSOS HUMANOS		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Bajo (De 3 a 6 meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Bajo (Entre 99.999 y 50.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA GESTIÓN DEL TALENTO HUMANO PLANEACIÓN GESTIÓN DE LA COMUNICACIÓN LAS DEMÁS ÁREAS	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			
El alcance de la ejecución del proyecto incluye: La integración e implementación del Plan de Sensibilización y Capacitación de seguridad y Privacidad de la información con el Plan Institucional de Capacitación - PIC vigente en El Organismo.			
POTENCIALES BENEFICIOS ESPERADOS			
*Todos los empleados del Fondo, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo en el marco de seguridad y privacidad de la información.			
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS			
*Porcentaje de ejecución del cronograma del proyecto			
PROYECTOS RELACIONADOS			
P1-- ESTABLECIMIENTO DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.			
COMPONENTE DE GOBIERNO EN LÍNEA			
*Seguridad y Privacidad de la Información			
ALINEAMIENTO ESTRATÉGICO SECTORIAL			
*PETI			
FACTORES CRÍTICOS DE ÉXITO			
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva			
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo		
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información		

6.3. Alistamiento y Consecución de Datacenter.

ALISTAMIENTO Y CONSECUCIÓN DE DATACENTER	
OBJETIVOS DEL PROYECTO	Este servicio le permitirá al Fondo, realizar una mejor organización y optimización de sus servicios del centro de datos, el cual debe estar cubierto y soportado por el área interna de TI.
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.18. –5.1.19.–5.1.20 SEGURIDAD DE LAS OPERACIONES 5.1.23. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 5.1.9.-5.1.24. CUMPLIMIENTO

TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Muy Alto (Mayor a 1 año)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Muy Alto (Mayor a 400.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA SECRETARÍA GENERAL GESTIÓN DE LA COMUNICACIÓN	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			
Alcance: Se llevara a cabo un servicio completo para los servicios del centro de datos, sus recursos físicos y lógicos los cuales le permiten soportar la infraestructura tecnológica del Fondo, se deben hacer y presentar los requerimientos necesarios para ello.			
POTENCIALES BENEFICIOS ESPERADOS			
* Implementar Microsoft System Center * Implementar servicios de herramienta de backup Data Protection Manager * Mejorar los servicios de infraestructura tecnológica del Fondo * Identificar del software instalado * Identificar componentes tecnológicos, sistemas, versiones y estado de licenciamiento			
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS			
*Porcentaje de ejecución del cronograma del proyecto			
PROYECTOS RELACIONADOS			
P2 - INTEGRACIÓN DEL PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON EL PIC P7 - IMPLEMENTACIÓN MODULO SGSI EN LA HERRAMIENTA ISOLUCIÓN			
COMPONENTE DE GOBIERNO EN LÍNEA			
*Seguridad y Privacidad de la Información			
ALINEAMIENTO ESTRATÉGICO SECTORIAL			
*PETI			
FACTORES CRÍTICOS DE ÉXITO			
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva			
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo		
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información		

6.4. Continuidad del Negocio SGSI.

CONTINUIDAD DEL NEGOCIO	
OBJETIVOS DEL PROYECTO	Prestar los servicios profesionales especializados para asesorar, planear, ejecutar y monitorear el proyecto correspondiente a la formulación de un plan de continuidad de negocio en sus fases de diseño, brindando el acompañamiento para la formulación de las acciones institucionales que permitan desarrollar la un modelo de gestión de continuidad de negocio formal BCP al interior de la entidad.
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.24. CONTINUIDAD DEL NEGOCIO SEGURIDAD DE LA INFORMACIÓN

TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Alto (9 A 12 Meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Alto (Entre 399.999 y 200.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA PROCESOS MISIONALES DIRECCIÓN	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			
Teniendo en cuenta los antecedentes expuestos por El Organismo, El Fondo ha identificado la necesidad de llevar a cabo el desarrollo de un plan de continuidad de negocio alineado a las mejores prácticas y estándares. Un plan de continuidad de negocio es un conjunto de procedimientos y de información la cual es desarrollada, implementada y preparada para usarla en un evento de emergencia o desastre. Por lo tanto, la continuidad del negocio es el proceso que asegura que una organización puede sobrevivir a un evento que cause interrupción al normal funcionamiento del negocio. En miras de cumplir el objetivo de mantener la continuidad del negocio surge la necesidad de definir un modelo de continuidad en El Organismo.			
POTENCIALES BENEFICIOS ESPERADOS			
* Contar con un BCP que permita garantizar la continuidad de los servicios misionales de la ESAP. * identificar los servicios críticos de la ESAP. * Identificar los riesgos que afecten la continuidad del negocio (BCP).			
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS			
*Porcentaje de ejecución del cronograma del proyecto			
PROYECTOS RELACIONADOS			
P1 - ESTABLECIMIENTO DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.			
COMPONENTE DE GOBIERNO EN LÍNEA			
*Seguridad y Privacidad de la Información			
ALINEAMIENTO ESTRATÉGICO SECTORIAL			
*PETI			
FACTORES CRÍTICOS DE ÉXITO			
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva			
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo		
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información		

6.5. Plan de Recuperación de Desastres.

PLAN DE RECUPERACIÓN DE DESASTRES-PRD			
OBJETIVOS DEL PROYECTO	Acompañar al Organismo en la formulación de las acciones institucionales que permitan desarrollar la un Plan de Recuperación de Desastres DRP a su interior.		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.24. CONTINUIDAD DEL NEGOCIO SEGURIDAD DE LA INFORMACIÓN		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Alto (9 A 12 Meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Alto (Entre 399.999 y 200.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta

ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA DIRECCIÓN	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA

DESCRIPCIÓN/ALCANCE
Teniendo en cuenta los antecedentes expuestos por El Organismo, El Fondo ha identificado la necesidad de llevar a cabo el desarrollo de un plan de recuperación de desastres alineado a las mejores prácticas y estándares. El DRP (Disaster Recovery Plan o Plan de recuperación de desastres) es la estrategia que tiene planteada la entidad para restablecer los servicios de TI (Hardware y Software) a cargo de este Organismo, después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, daño premeditado, ataque de cualquier tipo el cual atente contra la continuidad del negocio. Después de fortalecer la infraestructura tecnológica como se ha hecho esta entidad durante las últimas vigencias. Se ha identificado que cuando no se cuenta con un DRP implementado y se tiene una eventualidad, los encargados de la operación tecnológica tratan de recuperar la operación de los servicios que se prestan a cualquier costo, ya que, dependen del funcionamiento de sus sistemas de información. El objetivo de esta consultoría es formular el Plan de Recuperación de Desastres para la infraestructura tecnológica del Fondo. Beneficios del DRP para El Fondo: Algunos de los beneficios al hacer un DRP, a parte de los ahorros del esfuerzo, tiempo y dinero son: · -Mantener la continuidad de los servicios relacionados con la TIC · -Proteger a la entidad de fallas generales en los servicios informáticos. · -Minimizar los riesgos generados por la falta de servicios. · -Garantizar el acceso de la información institucional. · -Mantener la disponibilidad de los recursos informáticos. · -Minimizar la toma de decisiones erróneas al presentarse algún desastre. · -Dar atención continua a los clientes, proveedores, accionistas, colaboradores. · -Tener capacidad de recuperación exitosa.
POTENCIALES BENEFICIOS ESPERADOS
* Contar con un Plan de Recuperación de Desastres - DRP * Definir estrategias de desastre para la recuperación de los servicios tecnológicos y misionales del Fondo.
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS
*Porcentaje de ejecución del cronograma del proyecto
PROYECTOS RELACIONADOS
P1 - ESTABLECIMIENTO DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
COMPONENTE DE GOBIERNO EN LÍNEA
*Seguridad y Privacidad de la Información
ALINEAMIENTO ESTRATÉGICO SECTORIAL
*PETI
FACTORES CRÍTICOS DE ÉXITO
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva

CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información

6.6. Pruebas Ethical Hacking.

PRUEBAS ETHICAL HACKING			
OBJETIVOS DEL PROYECTO	Realizar dos (2) pruebas en el año de Ethical Hacking		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.18. –5.1.19.–5.1.20. SEGURIDAD DE LAS OPERACIONES 5.1.9.-5.1.24. CUMPLIMIENTO		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Alto (9 A 12 Meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Alto (Entre 399.999 y

			200.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁ TICA
DESCRIPCIÓN/ALCANCE			
Realizar dos (2) pruebas en el año de Ethical Hacking a toda la infraestructura crítica de la entidad, con personal certificado y amplia experiencia en este tipo de labores.			
POTENCIALES BENEFICIOS ESPERADOS			
* identificar y mitigar las brechas de seguridad de los componentes tecnológicos del Fondo.			
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS			
*Porcentaje de ejecución del cronograma del proyecto			
PROYECTOS RELACIONADOS			
P2 - INTEGRACIÓN DEL PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON EL PIC.			
COMPONENTE DE GOBIERNO EN LÍNEA			
*Seguridad y Privacidad de la Información			
ALINEAMIENTO ESTRATÉGICO SECTORIAL			
*PETI			
FACTORES CRÍTICOS DE ÉXITO			
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva			
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo		
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información		

6.7. - Implementación Módulo SGSI en la Herramienta Isolución.

IMPLEMENTACIÓN MÓDULO SGSI EN LA HERRAMIENTA ISOLUCIÓN			
OBJETIVOS DEL PROYECTO	Suministrar una herramienta de Software en Cloud u On Premise para el manejo del ciclo de vida del SGSI del Organismo.		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	EVALUACIÓN Y DESEMPEÑO 5.1.18. –5.1.19.–5.1.20. SEGURIDAD DE LAS OPERACIONES 5.1.9.-5.1.24. CUMPLIMIENTO 5.1.21. GESTIÓN DE ACTIVOS 5.1.23. GESTIÓN INCIDENTES DE SEG. DE LA INFORMACIÓN		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Alto (9 A 12 Meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Muy Alto (Muy Alto (Mayor a 400.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA PLANEACIÓN LAS DEMÁS ÁREAS	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			

Realizar la implementación del Módulo del Sistema de Gestión de Seguridad de la Información en la herramienta Isolución, permitiendo contar con una gestión unificada para el almacenamiento de los documentos pertinentes al SGS.
POTENCIALES BENEFICIOS ESPERADOS
* Contar con un software que permita llevar el ciclo de vida del SGSI. * Almacenar, publicar, gestionar y comunicar los documentos del SGSI de forma centralizada y en un entorno web.
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS
*Porcentaje de ejecución del cronograma del proyecto
PROYECTOS RELACIONADOS
P2 - INTEGRACIÓN DEL PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON EL PIC P3 - AFINAMIENTO DE DATACENTER
COMPONENTE DE GOBIERNO EN LÍNEA
*Seguridad y Privacidad de la Información
ALINEAMIENTO ESTRATÉGICO SECTORIAL
*PETI
FACTORES CRÍTICOS DE ÉXITO
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto. *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva

CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información

6.8. Desarrollo e Implementación de Ambientes Virtuales en el Organismo.

DESARROLLO E IMPLEMENTACIÓN DE AMBIENTES VIRTUALES EN EL ORGANISMO			
OBJETIVOS DEL PROYECTO	Realizar el desarrollo e implementación de herramientas para ambientes virtuales de Aprendizaje para El fondo.		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.16.-5.1.17. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Alto (9 A 12 Meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Alto (Entre 399.999 y 200.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA PLANEACIÓN LAS DEMÁS ÁREAS	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			
El alcance de la ejecución del proyecto incluye: * Aplicación online para evaluación de Calidad de los Recursos Tecnológicos del Fondo * Gestión de recursos tecnológicos (online)- Ecosistema Tecno-laboral * Plataforma virtual en Línea * Portal Virtual del Trabajador.			
POTENCIALES BENEFICIOS ESPERADOS			
*Implementar estrategias pedagógicas para lograr la apropiación, uso y aplicación de las tecnologías de la información y la comunicación (TIC) por parte de los trabajadores del Fondo. *Contar con un portal virtual de los trabajadores, para brindarles servicios en línea, de manera fácil y rápida. *Brindar más servicios informativos y formativos en línea, para llegar a todos los interesados *Contar con una aplicación online para realizar la evaluación de calidad de los recursos formativos producidos por El Fondo y también los externos.			

INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS	
*Porcentaje de ejecución del cronograma del proyecto	
PROYECTOS RELACIONADOS	
P3 - ALISTAMIENTO DE DATACENTER	
COMPONENTE DE GOBIERNO EN LÍNEA	
*Seguridad y Privacidad de la Información	
ALINEAMIENTO ESTRATÉGICO SECTORIAL	
*PETI	
FACTORES CRÍTICOS DE ÉXITO	
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto . *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva	
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información

6.9. Migración IPV4 A IPV6.

MIGRACIÓN IPV4 A IP6			
OBJETIVOS DEL PROYECTO	Realizar la migración de IPv4 a IPv6 de los componentes tecnológicos del Fondo.		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.4.- 5.1.5.- 5.1.6.-5.1.7.- 5.1.8. SEG. COMUNICACIONES		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Alto (9 A 12 Meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Muy Alto (Muy Alto (Mayor a 400.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			
Realizar un diagnóstico, plan de implementación y monitoreo del proceso de transición de IPv4 a IPv6 a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información.			
POTENCIALES BENEFICIOS ESPERADOS			
*El nuevo protocolo IPv6 Incorpora mecanismos de cifrado de los paquetes con Ipsec *Mecanismos de seguridad avanzada sobre los datos transmitidos *Mejora de las capacidades de autenticación y privacidad de los datos que transmite porque los paquetes que proceden de un origen			
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS			
*Porcentaje de ejecución del cronograma del proyecto			
PROYECTOS RELACIONADOS			
P3 - ALISTAMIENTO DE DATACENTER			
COMPONENTE DE GOBIERNO EN LÍNEA			
*Seguridad y Privacidad de la Información			
ALINEAMIENTO ESTRATÉGICO SECTORIAL			
*PETI			
FACTORES CRÍTICOS DE ÉXITO			
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto. *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva			
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo		

LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información

6.10. Mantenimiento de Control de Acceso.

MANTENIMIENTO DE CONTROL DE ACCESO			
OBJETIVOS DEL PROYECTO	Realizar mantenimiento correctivo y preventivo a los molinetes de las entradas del Fondo.		
DOMINIOS DE LA NTC/ISO 27001 RELACIONADOS	5.1.13. CONTROL DE ACCESO		
TIEMPO APROXIMADO DE IMPLEMENTACIÓN	Alto (9 A 12 Meses)	COSTO APROXIMADO DE IMPLEMENTACIÓN	Alto (Entre 399.999 y 200.000). Miles de Pesos-$
GRADO DE URGENCIA DE LA IMPLEMENTACIÓN	Alta	GRADO DE IMPLICACIONES	Alta
ÁREAS INTERESADAS/STAKEHOLDERS	GESTIÓN TECNOLÓGICA	SUPERVISIÓN DEL PROYECTO	COORDINACIÓN DE SISTEMAS E INFORMÁTICA
DESCRIPCIÓN/ALCANCE			
Realizar manteamientos correctivos y preventivos a los molinetes de las entradas de la ESAP, con el fin de garantizar su correcto funcionamiento y permitir el ingreso a la a entidad a los funcionarios, contratistas, visitantes y demás servidores.			
POTENCIALES BENEFICIOS ESPERADOS			
*Afinamiento a los dispositivos biométricos de control de acceso *Mantenimiento preventivo y correctivo a los dispositivos y molinetes de la entrada *Depuración de usuarios de la base de datos			
INDICADORES BÁSICOS PARA EL LOGRO DE LOS OBJETIVOS			
*Porcentaje de ejecución del cronograma del proyecto			
PROYECTOS RELACIONADOS			
P1-ESSTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
COMPONENTE DE GOBIERNO EN LÍNEA			
*Seguridad y Privacidad de la Información			
ALINEAMIENTO ESTRATÉGICO SECTORIAL			
*PETI			
FACTORES CRÍTICOS DE ÉXITO			
*Financiamiento *Recursos para la ejecución y desarrollo del proyecto. *Compromiso de las áreas interesadas *Apoyo de la Administración Central y Junta directiva			
CAPACIDADES DE TI	Recurso Humano - Recurso Técnico - Tiempo		
LIDER DEL PROYECTO	Coordinador de Tecnologías de la Información		