MSPI

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARAUCA – ARAUCA

2024

Contenido

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI) muestra los lineamientos y orienta la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), la integración con el Programa Integral de Protección de Datos Personales y la Gestión de Riesgos de Seguridad de las instituciones públicas. El Instituto de Desarrollo de Arauca - IDEAR en el desarrollo de sus actividades ha identificado la necesidad de implementar el modelo dentro de su misión con el fin de salvaguardar la información a través de proyectos e iniciativas estratégicas que garanticen sus pilares de confidencialidad, integridad y disponibilidad.

El presente busca no solo cumplir con los estándares nacionales e internacionales en materia de seguridad de la información, sino también alinearse a las políticas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) de Colombia. En un contexto donde la protección de los datos se erige como un componente esencial para el desarrollo sostenible y la confianza ciudadana, este modelo se posiciona como una herramienta estratégica para fortalecer la integridad, disponibilidad y confidencialidad de la información en manos de la institución.

La adopción de este Modelo no solo responde a un cumplimiento normativo, sino que se erige como un compromiso activo hacia la construcción de una institución pública sólida, transparente y orientada a proteger los intereses de sus usuarios y colaboradores. En este sentido, la creación de un entorno seguro para la gestión de datos financieros y personales se convierte en un imperativo ético y operativo, asegurando la continuidad de la misión institucional y generando un valor añadido en términos de confianza y legitimidad.

2. OBJETIVO

Definir e implementar las actividades del Plan de Seguridad y Privacidad de la Información alineadas con la NTC/IEC ISO 27001:2013 y la estrategia de Gobierno Digital, de acuerdo con sus habilitadores y con el fin de fortalecer sus pilares y reducir los riesgos inherentes a la seguridad digital.

3. ALCANCE

El Modelo de Seguridad y Privacidad de la Información - MSPI - al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la Estrategia de Seguridad Digital de la institución, tiene como alcance la aplicabilidad dentro de todos los procesos definidos dentro del IDEAR, al igual que sus activos, tanto tangibles como intangibles.

4. MARCO NORMATIVO

El Modelo de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

1. Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.

2. Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

3. Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Regla

4. Decreto 1499 de 2017, Modelo de Integración de Planeación y Gestión -MIPG. En cada una de las entidades se integrará un comité institucional de gestión y desempeño encargado de orientar la implementación y operación del modelo integrado de planeación y gestión MIPG, el cual sustituirá los demás comités que tengan relación con el modelo y que no sean obligatorios por mandato legal.

5. Documento CONPES 3854 de 2016. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.

6. Decreto 1083 de 2015. Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014 que establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital).

7. Ley 527 de 1999, se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones

8. Ley 1712 de 2014

9. Ley 1581 de 2012.

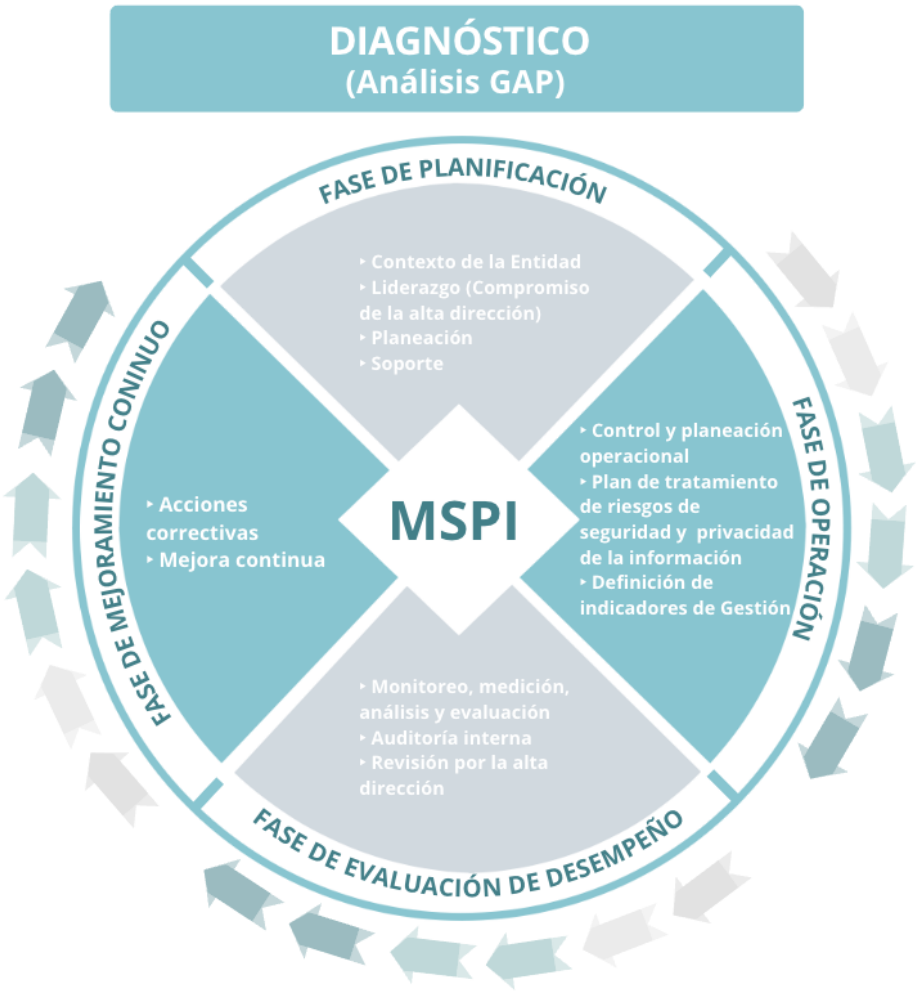
10. Manual de Gobierno Digital – MINTIC.

11. Modelo de Seguridad y Privacidad de la Información – MINTIC.

5. MODELO MSPI

El MSPI del Instituto de Desarrollo de Arauca - IDEAR toma como referencia el ciclo definido en el Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y Comunicaciones, el cual está basado en el ciclo PHVA conforme al estándar internacional ISO/IEC 27001:2022 y cuenta con 5 fases (Diagnóstico, Planificación, Implementación, Evaluación de Desempeño y Mejora Continua) que se describirán a continuación:

Gráfica 1.
Modelo MSPI



Nota: MSPI del MINTIC

5.1. Fase Diagnóstico

Dentro del contexto del planteamiento de un Sistema de Gestión de Seguridad y Privacidad de la Información conforme al MSPI y al ciclo de PHVA establecido, así como del Programa Integral de Gestión de Datos Personales y de la Gestión de Riesgos de Seguridad de la Información. Se plantea como primera fase en su ejecución un diagnóstico actual de la implementación previa de planes y políticas que sean precursoras del plan maestro aquí expuesto, con ello se realizó una evaluación de cada ítem expuesto en el artefacto publicado por MINTIC en su política de gobierno digital que tiene 3 principales componentes para su evaluación:

Gráfico 2:
Fase de diagnóstico

Nota: MSPI del MINTIC

Siguiendo el modelo, se realizan las siguientes actividades con el fin de cumplir las 3 actividades previstas en la fase de diagnóstico:

- Levantamiento de información: En esta fase se recopilaron documentos en los que se detallan procesos en los que se incluye la Misión, mapas de procesos y de riesgos, plan de continuidad, controles sobre riesgos asociados a la contratación de personal.

- Relación de áreas involucradas: Relacionamiento con líneas de procesos, temas y responsables de las actividades desarrolladas por la institución.

- Identificación de la línea base de seguridad administrativa y técnica: Allí se evaluaron según la escala de evaluación propuesta por las Mintic sobre cada uno de los aspectos administrativos, tecnológicos y PHVA relacionados con políticas, procedimientos, roles y controles que se relacionan con seguridad de la información e infraestructura tecnológica.

5.1.1. Ejecución del diagnóstico

5.1.1.1. Contexto y estado actual de la institución:

Misión:

La Misión del Instituto de Desarrollo de Arauca - IDEAR, consiste en contribuir con el fomento del desarrollo económico y bienestar social del Departamento de Arauca, a través de la ejecución de las actividades financieras y gestión de programas y proyectos de inversión que, en el marco legal vigente, puede desplegar como establecimiento público del orden territorial y su categoría de instituto para el financiamiento y desarrollo territorial, INFIS.

Visión:

El Instituto de Desarrollo de Arauca, IDEAR, se consolidará como una entidad líder del nivel descentralizado departamental, consecuencia de la implementación de su modelo de gestión y financiamiento de proyectos socioeconómicos, que promuevan el bienestar de la región y garantice su sostenimiento con rentabilidad en el contexto social e institucional.

Objetivos Estratégicos:

- Fortalecer la capacidad financiera del Instituto a través del portafolio de servicios.
- Promover, financiar, asesorar e invertir en proyectos de impacto social que contribuyan al desarrollo económico y social del Departamento de Arauca.
- Fortalecer el desarrollo institucional buscando alcanzar niveles óptimos de eficiencia en las actividades planificadas.
- Optimizar el nivel de efectividad del control de la gestión institucional y las líneas de defensa del instituto.
- Incrementar el nivel de competencias y la calidad de vida de los colaboradores, las expectativas y necesidades de los clientes del instituto.

Metas institucionales:

Tabla 1:

Metas institucionales

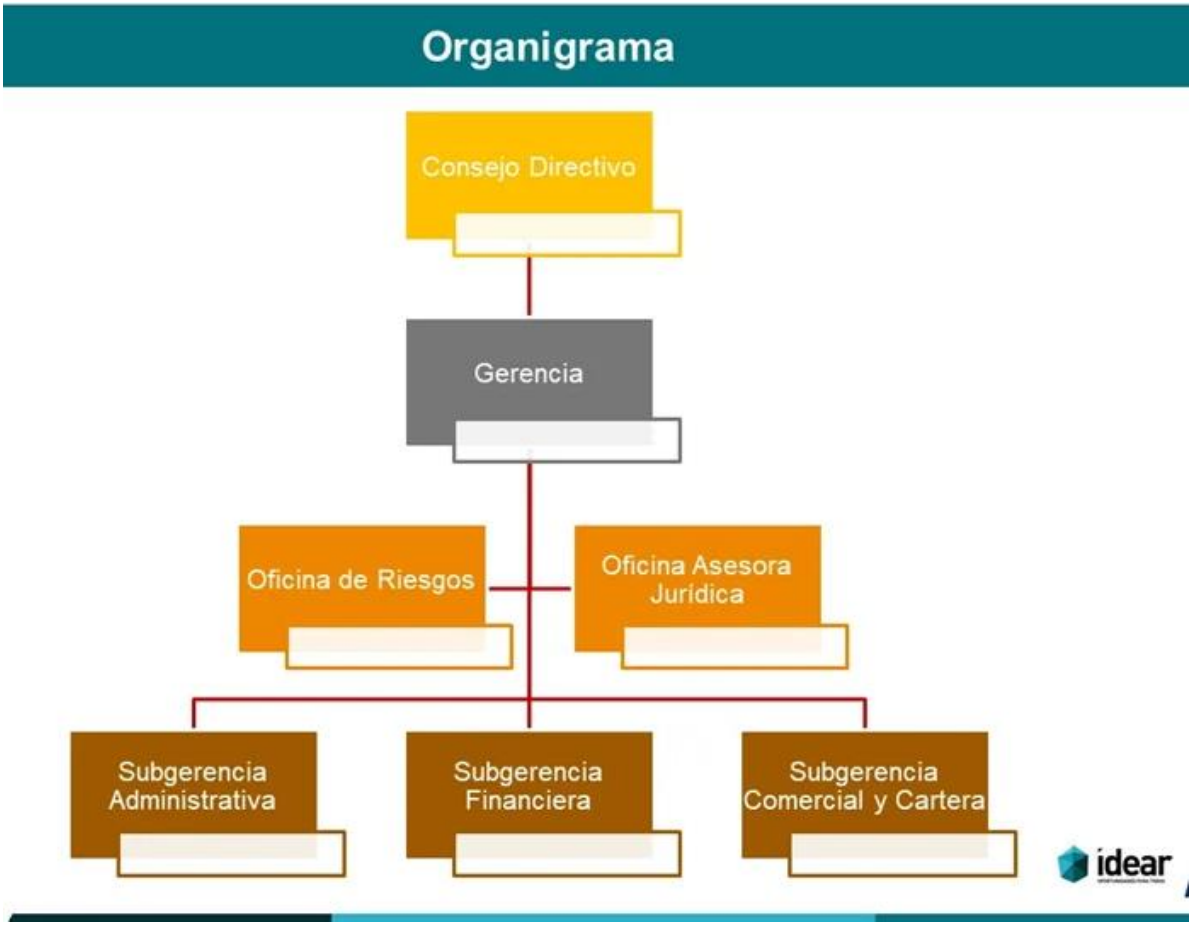
Meta		
ID	Nombre	Medición actual Tercer trimestre 2023
1	Asignar recursos a través de la línea de crédito educativa, orientados a financiar los costos totales o parciales de matrícula ordinaria, sostenimiento y/o trabajo de grado de programas de educación superior avalados por el Estado en modalidades presencial, semipresencial y a distancia ofrecidos en el país por instituciones educativas debidamente registradas en el Sistema Nacional de Información de Educación Superior – SNIES, al igual que para el estudio de lenguas extranjeras, pregrado y posgrado fuera del país.	72%
2	Financiar créditos a los municipios y entidades públicas descentralizadas del orden municipal y departamental, destinados al apoyo y cumplimiento de los planes de desarrollo y proyectos de inversión, así como solventar necesidades puntuales de liquidez. (Crédito Institucional)	190%
3	Financiar créditos de corto plazo recursos a los contratistas del municipio, departamento y sus descentralizadas, mediante el endoso de las actas de obras ejecutadas o facturas de servicios prestados. Dicha operación se efectuará en un porcentaje del valor del acta o factura de venta sobre el valor neto (Descuentos de Actas y Facturas)	0%
4	Asignar recursos a través de Operador a personas naturales y jurídicas, para atender sectores como el agropecuario, industrial, comercio y servicios.	45%
5	Financiar Créditos de Libranza a servidores públicos de entidades que tengan su sede en el Departamento de Arauca y a empleados de empresas privadas que presten servicios públicos, para libre destinación.	71%
6	Asignar Créditos de Inversión a particulares que prestan servicios públicos, para impulsar programas de desarrollo regional rural y urbano mediante la financiación y asesoría, así como proyectos de inversión en los sectores económico y social.	125%
7	Ejecutar el recaudo efectivo de la Cartera. Cumplir el 91% de la meta proyectada de recuperación de cartera para la vigencia 2023.	72%
8	Mantener consolidada la información de los procesos jurídicos, ejecutivos y ordinarios tendientes a la recuperación de Cartera.	75%
9	Ofertar para venta el 58% de los bienes inmuebles del instituto.	50%
10	Fortalecer la Gestión Estratégica del IDEAR: Evaluar el Sistema de Control Interno y Gestión Institucional mediante FURAG.	100%
11	Fortalecer la Gestión estratégica del IDEAR: Aplicar los instrumentos de Gestión Documental del Idear (TRD, TVD, PGD, PINAR, SIC, FUID, CCD).	25%
12	Aplicar los Sistemas de Administración de Riesgos en el Instituto SARM, SARC, SARO, SARL, SARLAFT.	75%

Nota: Elaboración propia

Estructura organizacional:

Gráfico 3:

Estructura organizacional



Fuente: tomado del Decreto Ordenanzal 723/2017

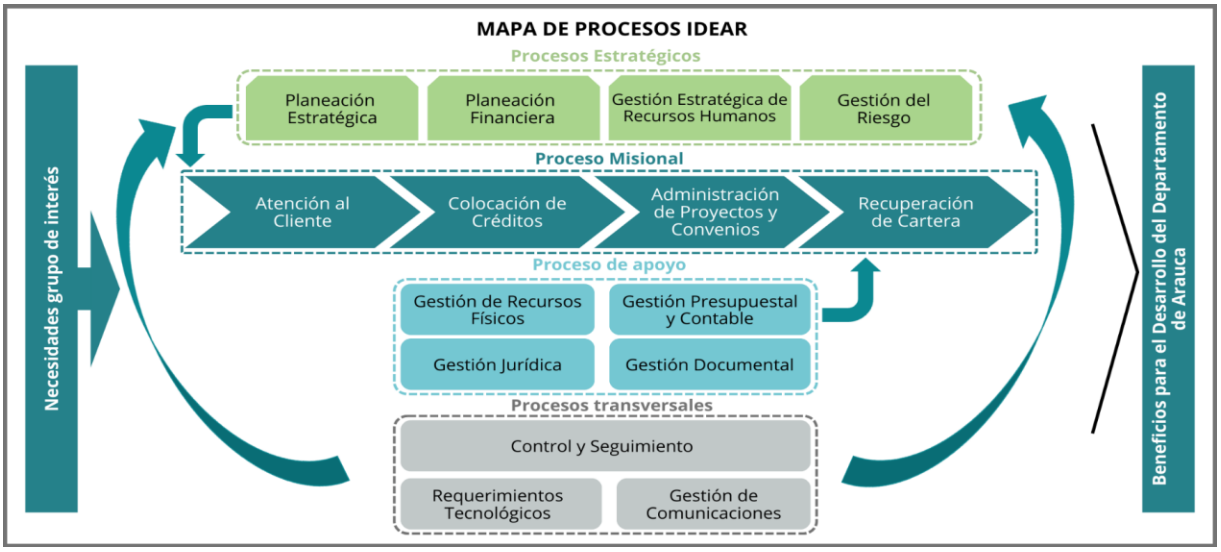
La entidad cuenta con 6 áreas: Gerencia, Oficina de Riesgos, Oficina asesora Jurídica, , Subgerencia administrativa, Subgerencia Financiera y Subgerencia comercial y de cartera.

El recurso humano está conformado por 34 funcionarios de planta y 14 funcionarios vinculados a la entidad con órdenes de prestación de servicios (Contratos de OPS).

Modelo Operativo:

Gráfico 4:

Mapa de procesos



Nota: Tomado de manual de procesos y procedimientos. IDEAR. Versión 01

Procesos Estratégicos:

Tabla 2:

Procesos estratégicos

ID	Nombre	Objetivo
1	Proceso de planeación estratégica	Garantizar una eficaz planificación del instituto de Desarrollo de Arauca IDEAR BASADO EN EL MODELO Integrado de Gestión y Planificación- MIPG
2	Proceso de planeación financiera	Administrar y controlar las inversiones financieras que realiza la entidad a través de operaciones en el mercado financiero para asegurar el respaldo de la rentabilidad del Instituto de Desarrollo de Arauca- IDEAR
3	Proceso de gestión del riesgo	Direccionar al Instituto de Desarrollo de Arauca- IDEAR hacia una cultura de identificación, administración, control, y mitigación de los riesgos financieros, velando por el buen funcionamiento y la liquidez del instituto
4	Proceso gestión estratégica del talento humano	Establecer un proceso que administre el ciclo del personal al interior del instituto y que garantice el fortalecimiento del Talento Humano mediante, programas y planes que desarrollen integralmente a los servidores públicos en beneficio del cumplimiento de la misión del instituto de Desarrollo de Arauca- IDEAR

Nota: Tomado de manual de procesos y procedimientos. IDEAR. Versión 01.

Procesos Misionales:

Tabla 3:

Procesos misionales

ID	Nombre	Objetivo
1	Proceso atención al cliente	Garantizar el mejor trato al cliente con la información dada de los servicios del portafolio del instituto, gestión de los trámites de peticiones, quejas y reclamos y de la medición de satisfacción del cliente
2	Proceso de colocación de créditos	Establecer la metodología para la colocación de recursos del portafolio de servicios del instituto, las líneas son: Descuentos de actas y facturas; Educativo; Fomento público; Tesorería; Comerciales y libranza
3	Proceso administración de proyectos y convenios	Administrar recursos financieros de proyectos específicos, a través de cuentas convenio o contratos de mandato y formulación y ejecución de proyectos de asociaciones Público- privadas que realicen los usuarios en el territorio
4	Proceso de recuperación de cartera	Establecer la metodología y controles necesarios para que los recursos colocados en créditos retornen oportunamente al IDEAR.

Nota: Tomado del manual de procesos y procedimientos - IDEAR. Versión 01.

Procesos de Apoyo:

Tabla 4:

Procesos de apoyo

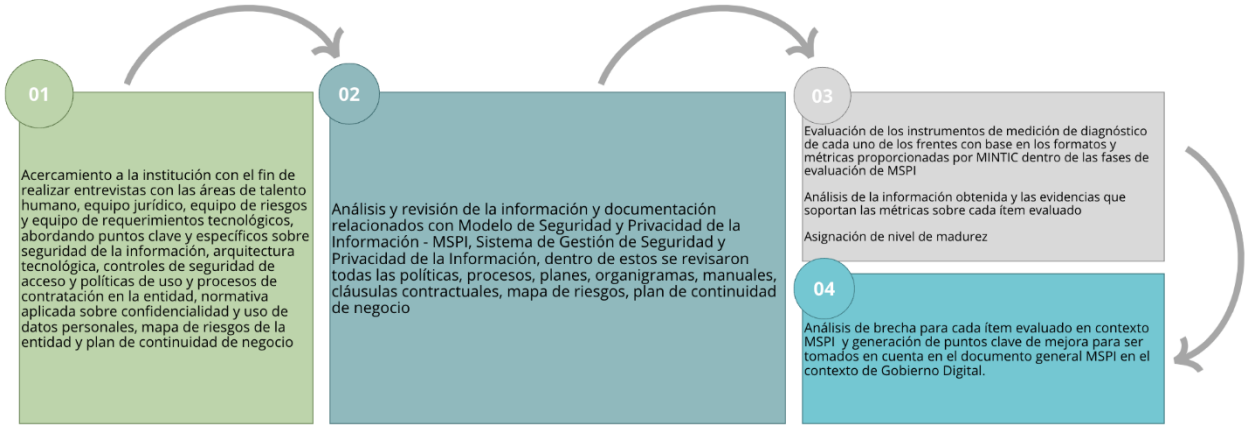
ID	Nombre	Objetivo
1	Proceso de gestión de recursos físicos	Garantizar el efectivo control de los activos de consumo, devolutivos y conservación de los bienes inmuebles, además del mantenimiento de la infraestructura del instituto.
2	Proceso de gestión jurídica	Defender los derechos e intereses del instituto. Prestar asesoría, gestionar, elaborar actos administrativos, que incidan directamente sobre las actividades legales y jurídicas con intervenciones oportunas.
3	Proceso de gestión presupuestal y contable	Garantizar una eficiente operación de los recursos de la empresa y suministrar la información requerida para la toma de decisiones en forma confiable y oportuna en el instituto.
4	Proceso de gestión documental	Gestionar la adecuada conservación de los documentos, mediante actividades administrativas y técnicas, tendientes a la planificación, manejo y organización de la documentación producida y recibida por la entidad, desde su origen hasta su destino final.

Nota: Tomado del manual de procesos y procedimientos - IDEAR. Versión 01.

5.1.1.2. Identificación de la madurez:

Con el fin de realizar la identificación del nivel de madurez en el que se encuentra la institución, se implementó el instrumento de diagnóstico propuesto por el MINTIC el cual permite evidenciar el nivel en el que los controles de seguridad de la información que presenta la institución al igual que el estado actual tanto de la gestión de seguridad y privacidad dentro de la entidad como el cumplimiento con la legislación vigente relacionada con protección de datos personales. Este diagnóstico se realizó de la siguiente manera:

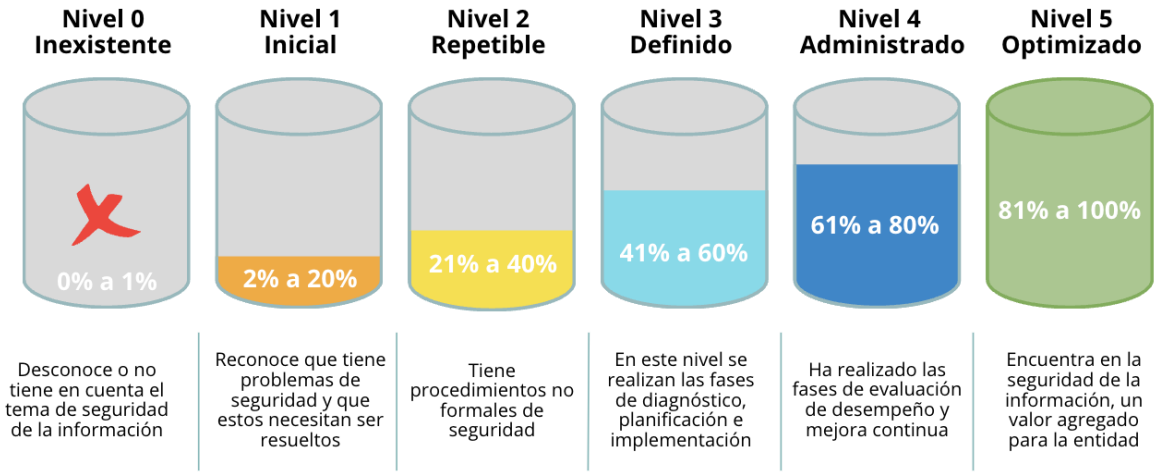
Gráfico 5:
Identificación de madurez



Nota: Elaboración propia

En el contexto del Manual de Gobierno Digital y el MSPI propuesto por el MINTIC, la madurez en Seguridad y Privacidad de la Información dentro de las instituciones públicas se mide de la siguiente manera:

Gráfico 6:
Escala de medición



Nota: MSPI del MINTIC

Gráfico 7:
Nivel de cumplimiento MSPI

NIVEL DE CUMPLIMIENTO MSPI	
FASE	ACTUAL
Planificación	3%
Operación	0%
Evaluación de desempeño	0%
Mejora continua	0%

Nota: Elaboración propia

Este resultado nos permite concluir que se encuentra en el nivel Inicial, la entidad reconoce que tiene problemas de seguridad de la información y estos necesitan ser resueltos prontamente. La brecha identificada es la siguiente:

Gráfico 8:
Brecha Anexo a ISO 27001:2013

Nota: MSPI del MINTIC
Tabla 5:
Evaluación de efectividad de controles

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES	
DOMINIO	ACTUAL
Políticas de seguridad de la información	0%
Organización de la seguridad de la información	2%
Seguridad de los recursos humanos	29%
Gestión de activos	10%
Control de accesos	0%
Critpografia	0%
Seguridad fisica y del entorno	11%
Seguridad de las operaciones	20%
Seguridad de las comunicaciones	8%
Adquisicion, desarollo y mantenimiento de sistemas	0%
Relaciones con los proveedores	0%
Gestión de incidentes de seguridad de la información	0%
Aspectos de seguridad de la información de la gestión de la continuidad de negocio	7%
Cumplimiento	21,5%

Nota: Elaboración propia

5.1.1.3. Levantamiento de Información:

Como se mencionó anteriormente, el levantamiento de información consiste en la recopilación de documentación en los que se detallan procesos y demás actividades, evidencias y formatos relacionados con el Modelo de Seguridad y Privacidad de la Información, al igual que la identificación de los responsables de gestionar el modelo y velar que el diagnóstico se realice de manera satisfactoria.

El resultado se encuentra adjunto en el *Anexo 1. Diagnóstico del MSPI - Instituto de Desarrollo de Arauca (IDEAR) 2023.xlsx*. En las pestañas: LEVANTAMIENTO DE INFO. y ÁREAS INVOLUCRADAS.

5.1.2. Hallazgos relevantes

Dentro de los hallazgos más importantes dentro de la fase de diagnóstico sobre seguridad e la información en la entidad tenemos:

- Ausencia de un documento que especifique alguna política concerniente a seguridad de la información.
- Ausencia de una política de seguridad de la información utilizada para los procesos internos de la entidad
- Ausencia de un plan de gestión del ciclo de vida del dato
- Sistemas de información dentro de arquitectura *on premise* instaladas dentro de e las instalaciones del IDEAR y administradas por el equipo de requerimientos tecnológicos
- Ausencia de inventarios sobre activos de información de la entidad y falta de protocolos para el intercambio de información

- Planteamiento de matriz de riesgos
- Existencia de un GPO en el que se describen los planes de continuidad de negocio ante riesgos inherentes a la operación de la institución, incluidos desastres naturales.
- En cuanto a capacitación de funcionarios sobre seguridad de la información se evidencian flyers emitidos por el equipo de requerimientos tecnológicos en los que se explican algunas buenas prácticas para el uso y correcta disposición de información y tips sobre seguridad.
- Los funcionarios no son conscientes de los posibles riesgos asociados a la fuga de información y al inventario de activos que lleven a la organización a proteger sus datos personales, sensibles y sus repositorios de información.

5.2. Fase Planificación

Una vez finalizado el diagnóstico de la entidad respecto a su contexto en términos de privacidad y seguridad de la información, se procede a la fase de planificación, la cual de acuerdo a la norma ISO 27001:2022, comprende la identificación de las expectativas del gerencia de la organización; al igual que la definición de las responsabilidades y obligaciones de la alta dirección en relación con el sistema de gestión de seguridad de la información, incluida la necesidad de que la alta dirección prepare una política de seguridad de la información adecuada a IDEAR; el establecimiento de los requerimientos para la valoración y tratamiento de riesgos de seguridad, la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento; y finalmente, el soporte que establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información.

Gráfico 9:
Fase planificación

Nota:

5.2.1. Necesidades y expectativas

A continuación, se presentan las necesidades, requisitos y expectativas de las partes interesadas en la implementación y aseguramiento de una Política de Seguridad y Privacidad de la Información, dentro de la entidad.

Tabla 6:

Necesidades y expectativas

Partes Interesadas	Necesidades	Requisitos	Expectativas
Alta gerencia Instituto de Desarrollo de Arauca - IDEAR	Disponibilidad, integridad y confidencialidad de la información	Definir directrices y políticas ajustadas a las condiciones operacionales del instituto Cumplir con la normatividad aplicable	Determinar las normas aplicables para el MSPI Mejorar la imagen de la institucionalidad e incrementar el nivel de competitividad Cumplir con los requerimientos y las directrices establecidas por los diferentes entes gubernamentales
Funcionarios del Instituto de Desarrollo de Arauca - IDEAR	Disponibilidad, integridad y confidencialidad de la información Contar con herramientas aprobadas Conocer políticas de manejo de sus herramientas y la información que utilizan	Apoyo técnico y tecnológico que permita cumplir con las políticas establecidas en la Política de Seguridad y Privacidad de la Información Disponibilidad del Servicio Apoyo administrativo que permita cumplir con la normatividad establecida en la PSPI	Obtener cumplimiento de la disponibilidad para el apoyo requerido Conocer las políticas y procedimientos de acuerdo al MSPI, al igual que los cambios generados en el mismo Garantía de la confidencialidad e integridad de la información
Proveedores	Especificación es técnicas de lo requerido, acorde a las políticas de seguimientos del SGSI.	Acuerdos de confidencialidad que protejan la disponibilidad, integridad y confidencialidad de la información	Conocimiento del MSPI y su política con el fin de minimizar los riesgos inherentes a la confidencialidad de la información
Comunidad	Información	Facilidad en el acceso a la información pública de manera permanente (transparencia y acceso a la información)	Transparencia en el desarrollo de los procesos institucionales Garantía de la protección y confidencialidad de su información

Nota:

5.2.2. Liderazgo y compromiso

A través del artículo 133 de la ley 1753 de 2015 se creó el sistema de gestión el cual integra los sistemas los sistemas de desarrollo administrativo y gestión de calidad y deberá articularse con el sistema de control interno, para lo cual el modelo integrado de planeación y gestión – MIPG surge como el mecanismo que facilita dicha integración y articulación, de tal manera que permite el fortalecimiento de los mecanismo, métodos y procedimiento de gestión y control al interior de los organismos y entidades del estado. Las funciones del comité son:

- Aprobar y hacer seguimiento, por lo menos una vez al trimestre, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión -MIPG
- Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión -MIPG
- Proponer al Comité Sectorial de Gestión y el Desempeño Institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión -MIPG
- Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión.
- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
- Reglamentar la operación para el Comité Institucional de Gestión y Desarrollo y el Equipo Operativo.

- Las demás que tengan relación directa con la implementación, desarrollo y evaluación del Modelo.

La Alta Dirección del Instituto de Desarrollo de Arauca - IDEAR se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

Para esto y teniendo en cuenta lo anterior, el día 21 de diciembre de 2023 se crea el Comité Institucional de Gestión y Desempeño, el cual tiene como función asegurar la implementación y el desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. Esto se evidencia a través del acta y de la institución.

5.2.3. Planeación Estratégica

La planeación estratégica de seguridad de la información se enmarca en un portafolio de iniciativas alineadas a los objetivos y expectativas de los interesados dentro de la organización, llamado Plan Estratégico para la Seguridad y Privacidad de la Información. En el mismo, se definen los proyectos y productos logrados y ajustados a las necesidades estratégicas que tiene como objetivo lograr la implementación y el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI).

Este plan fue aprobado por el Comité Institucional de Gestión y Desempeño el día x. Se presenta a continuación:

Tabla 7:
Iniciativas del plan estratégico

Estrategia	Iniciativa	Producto Esperado
Gestión de la seguridad de la información	Iniciativa 1: Definición de la Política y Manual de Políticas para la Seguridad y Privacidad de la Información	Producto 1: Política General de Seguridad y Privacidad de la Información
	Iniciativa 2: Definición de Roles y Responsabilidades de Seguridad de la Información	Producto 2: Inventario de activos de información del Instituto
	Iniciativa 3: Inventario de activos de información	
Gestión de Riesgos	Iniciativa 1: Identificación, valoración y clasificación de riesgos asociados a la Seguridad y Privacidad de Información	Producto 1: Matriz de Riesgos de Seguridad y Privacidad de la Información
	Iniciativa 2: Definición del Plan de Tratamientos de Riesgos de Seguridad	Producto 2: Plan de Tratamientos de Riesgos de Seguridad
	Iniciativa 3: Definición de indicadores de gestión de la Política de Seguridad de la Información	Producto 3: Matriz de indicadores de gestión de la Política

Estrategia	Iniciativa	Producto Esperado
Comunicación y Sensibilización	Iniciativa 1: Definición del Plan de Comunicación y Sensibilización de las Políticas de Seguridad y Privacidad de la Información	Producto 1: Plan de Comunicación y Sensibilización de las Políticas de Seguridad y Privacidad de la Información
	Iniciativa 2: Realizar jornadas de sensibilización a los funcionarios de la entidad	Producto 2: Evidencias de las actividades desarrolladas
Implementación de Controles	Iniciativa 1: Definición de políticas de gestión de controles y los procedimientos para la gestión de activos	Producto 1: Políticas de gestión de controles y los procedimientos para la gestión de activos [Contenidas en la Política General de Seguridad y privacidad de la Información]
Gestión de Incidentes	Iniciativa 1: Definición y formalización de los indicadores de gestión de incidentes	Producto 1: Procedimiento para la gestión de riesgos de activos de seguridad de la información
	Iniciativa 2: Definición del procedimiento de gestión de incidentes de seguridad de la información	

Nota: Elaboración propia

Los resultados de los productos esperados se referencian a continuación:

- *Anexo 2: Política General de Seguridad y Privacidad de la Información.docx*
- *Anexo 3: Procedimientos Gestión seguridad de información.docx*
- *Anexo 4: Matriz de Riesgos de Seguridad y Privacidad de la Información.xlsx*
- *Anexo 5: Plan de Tratamientos de Riesgos de Seguridad.docx*
- *Anexo 6: Matriz de indicadores de gestión de la Política.xlsx*
- *Anexo 7: Plan de Comunicación y Sensibilización de las Políticas de Seguridad y Privacidad de la Información.docx*
- *Anexo 8: Procedimiento para la gestión de riesgos de activos de seguridad de la información.docx*
- *Anexo 9: Inventario de activos de información.xlsx*

Las evidencias de las actividades de socialización se irán adjuntando a medida que se desarrollen las actividades propuestas en el cronograma del plan de comunicación.

5.2.4. Plan de Comunicación y Sensibilización

El plan de comunicación y sensibilización en términos de Seguridad y Privacidad de la Información del IDEAR tiene como objetivo garantizar la transferencia de información, al igual que oficializar los roles y responsabilidades ligadas a la política digital a cada parte interesada en los procesos de la organización. El documento se encuentra adjunto en el *Anexo 7: Plan de Comunicación y Sensibilización de las Políticas de Seguridad y Privacidad de la Información.docx*

5.3. Fase Implementación

Con el fin de llevar a cabo las actividades planteadas en la fase de planificación, el MINTIC propone dentro de sus lineamientos el desarrollo de 3 actividades principales que indican que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información. Estas se describen a continuación:

Gráfico 10:
Fase de implementación

Nota: MSPI del MINTIC

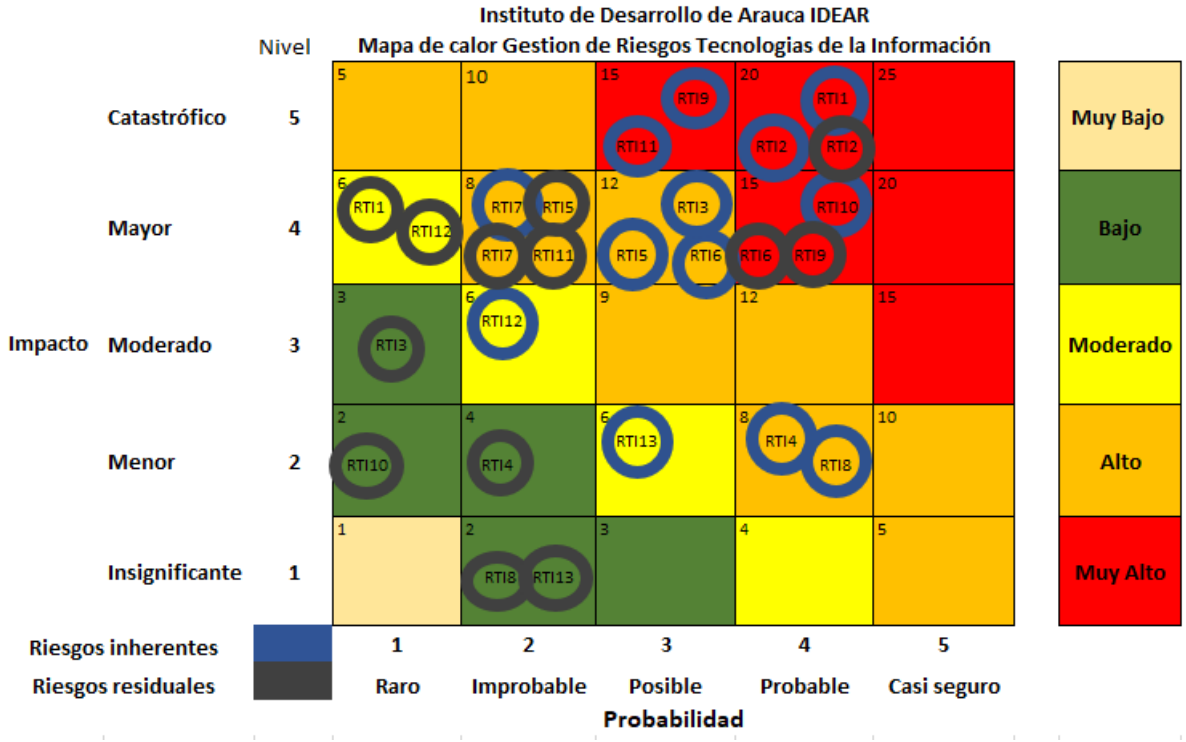
5.3.1. Control y planeación operacional

La implementación y operación del sistema gestión de seguridad y privacidad de la información se basa en la administración del riesgo de la seguridad de la información. Por esta razón, es imperativo el compromiso por parte del IDEAR en cuanto a la implementación de los controles procedimentales, tecnológicos y de talento humano que sean necesarios para llevar los riesgos de seguridad de la información a niveles aceptables.

Es por esto, y con el fin de definir un plan de tratamiento de riesgos que se identifican los riesgos dentro del contexto de seguridad y privacidad de la información inherente a los procesos desarrollados dentro de la entidad. Esta matriz se adjunta en el *Anexo 4: Matriz de Riesgos de Seguridad y Privacidad de la Información.xlsx.*

De esta forma, se concluye que el Instituto de Desarrollo de Arauca - IDEAR, presenta el siguiente perfil de riesgo:

Gráfico 11:
Mapa de calor Gestión de Riesgos Tecnologías de la Información



Nota: Elaboración propia

5.3.2. Plan de Tratamiento de Riesgos

El plan de tratamiento de riesgos del Instituto de Desarrollo de Arauca - IDEAR se encuentra como anexo en el siguiente documento, el se encuentra en proceso de aprobación: *Anexo 5: Plan de Tratamientos de Riesgos de Seguridad.docx.*

5.3.3. Definición de Indicadores de Gestión

La creación de indicadores de gestión está orientada principalmente a medir la eficacia, la eficiencia y la efectividad de las políticas y componentes del Marco de Seguridad y Privacidad de la Información dentro del Instituto de Desarrollo de Arauca - IDEAR, a través de métricas que servirán como insumos para el componente de mejora continua.

El documento fue construido tomando como referencia los lineamientos sobre indicadores de gestión para la seguridad de la información, del Ministerio de Tecnologías de Información y Comunicaciones – MINTIC.

5.3.3.1. Objetivo General

Medir la efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora.

5.3.3.2. Objetivos específicos

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la Gobernación.
- Servir como insumos al plan de análisis y tratamiento de riesgos.

5.3.3.3. Indicadores propuestos

A continuación, se definen los indicadores para medir la gestión y el cumplimiento en el Modelo de Seguridad y Privacidad de la Información. El consolidado total se encuentra en el *Anexo 6: Matriz de indicadores de gestión de la Política.xlsx.*

Tabla 8:
Indicadores propuestos

IDENTIFICADOR	NOMBRE
IND-SPI-001	INDICADOR 01 - POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
IND-SPI-002	INDICADOR 02 - ADOPCIÓN A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
IND-SPI-003	INDICADOR 03 - REVISIÓN POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
IND-SPI-004	INDICADOR 04 - ROLES Y RESPONSABILIDADES MSPI
IND-SPI-005	INDICADOR 05 - ACUERDOS DE CONFIDENCIALIDAD
IND-SPI-006	INDICADOR 06 - PLAN DE SENSIBILIZACIÓN
IND-SPI-007	INDICADOR 07 - INVENTARIO DE ACTIVOS
IND-SPI-008	INDICADOR 08 - CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
IND-SPI-009	INDICADOR 09 - TRATAMIENTOS DE EVENTOS RELACIONADOS MSPI
IND-SPI-010	INDICADOR 10 - LINEAMIENTOS DE ACCESOS Y DATACENTER
IND-SPI-011	INDICADOR 11 - PLAN DE AUDITORÍAS
IND-SPI-012	INDICADOR 12 - ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE

Nota: Elaboración propia

5.4. Fase Evaluación de Desempeño

De acuerdo con la guía estipulada por el MINTIC, para el modelo de seguridad y privacidad de la información. En esta cuarta fase, se establecen los aspectos a ser desarrollados por los responsables de la gestión de seguridad de la información en todos los niveles de la entidad, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.
En esta fase se establecen, principalmente, tres actividades que serán de valor para el modelo y que permiten aprovechar lo identificado en las fases predecesoras:

Gráfica 12:
Evaluación de desempeño

Nota: MSPI del MINTIC

5.4.1. Monitoreo y medición

Con el fin de verificar el desempeño de las políticas y procedimientos definidos en materia de la Seguridad y Privacidad de la Información, el Instituto de Desarrollo de Arauca - IDEAR, deberá desarrollar un conjunto de actividades de seguimiento donde se mantenga de manera continua la medición y verificación del cumplimiento de los aspectos planteados en la fase de Planificación del modelo y la forma como estas actividades se han ido desarrollando o ejecutando.

Para ello, la entidad deberá realizar: La revisión de sus controles y matriz de riesgo, el seguimiento a las actividades definidas, la medición de los indicadores planteados y la documentación de estos.

De acuerdo con la guía 16 del MSPI del MINTIC, cada una de estas actividades se compone de la siguiente manera:

5.4.1.1. Revisión:

- De la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.

- De la evaluación de los riesgos desarrollada en la entidad, donde a su vez se validan los niveles aceptables de riesgo y el riesgo residual después de la aplicación de controles y medidas administrativas.

5.4.1.2. Seguimiento:

Se deben programar las siguientes actividades:

- La programación y ejecución de las actividades de auditoría interna del MSPI
- La programación y ejecución de las revisiones por parte del encargado de seguridad y privacidad de la información.
- El alcance del MSPI y las mejoras de este.
- A los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o el desempeño de la seguridad y privacidad de la información.

5.4.1.3. Desarrollo de actividades:

Las siguientes actividades deben estar desarrolladas bajo el modelo de PHVA dentro de los procesos internos, logrando así una consolidación periódica de indicadores, con sus respectivas gráficas, análisis y evaluación de las no conformidades.

- Revisión de la eficacia del MSPI.
- Medición de la efectividad de los controles.
- Revisión de las valoraciones de los riesgos.
- Medición de los indicadores de gestión del MSPI.
- Realización de auditorías.
- Revisiones del MSPI por parte de la dirección.
- Actualizar los planes de seguridad.
- Registro de las actividades del MSPI.
- Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).

5.4.1.4. Documentación:

Todas las actividades de medición deben contar con su respectiva documentación, que permita llevar la trazabilidad de las actividades realizadas y que permita realizar las actualizaciones pertinentes en los siguientes documentos, con el fin de seguirle el hilo al contexto en el que la entidad se encuentra en todo momento:

- Eficiencia del MSPI
- Revisión de valoraciones de riesgos
- Actualización de los planes de seguridad
- Registro de actividades del MSPI
- Revisiones de acciones o planes de incidentes

Cada medición debe documentarse con al menos la siguiente información:

Tabla 9:
Guía de documentación de medición

NOMBRE MEDICIÓN	Aquí el nombre de la evaluación a realizar
OBJETIVO	El objetivo de la evaluación del indicador a realizar
ALCANCE	El alcance de la evaluación que se está realizando
ENTRADAS	¿Qué insumos se están utilizando para la medición?
ACTIVIDADES	Actividades realizadas para la evaluación
FRECUENCIA	¿Con qué frecuencia se está realizando la medición?
RESPONSABLE	Nombre y cargo del responsable
PROCEDIMIENTO RELACIONADO	Nombre del procedimiento realizado al indicador
OBSERVACIONES	Comentarios identificadas durante la evaluación
RESULTADO MEDICIÓN	Resultado de la medición/evaluación

Nota: Elaboración propia

5.4.2. Próximos pasos

Como próximos pasos, el Instituto de Desarrollo de Arauca - IDEAR, deberá apropiarse de las políticas, procedimientos generados para el Modelo de Seguridad y Privacidad de la Información, al igual que de la matriz de riesgos identificados, con el fin de realizar las mediciones de los indicadores planteados y poder medir la eficiencia y eficacia del MSPI.

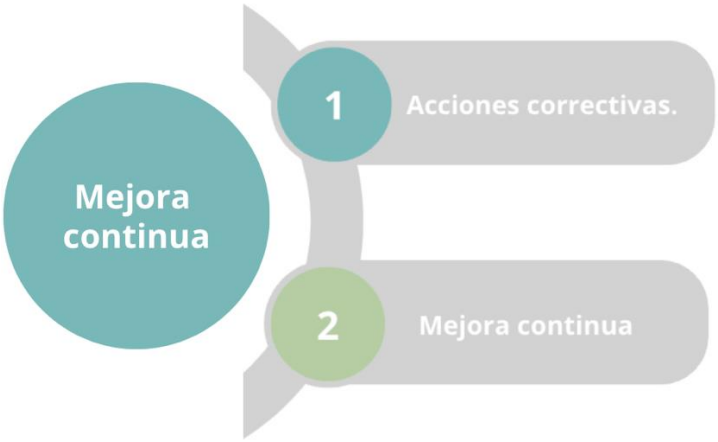
Para ello la entidad deberá:

1. Implementar las políticas y procedimientos definidos
2. Realizar las mediciones de los controles e indicadores planteados
3. Volver a realizar el diagnóstico de la entidad
4. Identificar la brecha
5. Realizar las acciones correctivas
6. Ajustar el MSPI de acuerdo con el contexto de la entidad
7. Repetir para entrar en la fase de mejoramiento continuo

5.5. Fase Mejora Continua

En esta quinta y última fase, el modelo pretende gestionar el mantenimiento y la mejora continua dentro del contexto de la seguridad y privacidad de la información de la entidad.

Gráfico 13:
Mejora continua



Nota: MSPI del MINTIC

La aplicación de esta fase le permitirá al IDEAR a partir de los resultados de la fase de evaluación, corregir de ser necesario, los errores cometidos, así como mejorar las acciones llevadas a cabo en las fases anteriores. Para ello, se deben tener presentes los siguientes conceptos:

- **Mejora Continua:** Es el procedimiento que tiene como finalidad buscar un mayor rendimiento de los procesos o actividades.
- **No conformidad:** Es el incumplimiento de un requisito.
- **Acciones correctivas:** Acción por medio de la cual se elimina la causa de la no conformidad, evitando que se repita.

5.5.1. Plan mejoramiento y comunicación de resultados

Para la implementación del plan de mejoramiento y así llevar a la entidad a una mejora continua, el equipo de control interno y el responsable del área TIC deberán trabajar en conjunto en la fase de evaluación de desempeño, y de acuerdo con los resultados, deberán identificar las no conformidades y las actividades correctivas necesarias, teniendo en cuenta los siguientes aspectos:

- En caso de presentarse no conformidades en las auditorías realizadas, el IDEAR deberá llevar a cabo las acciones necesarias para controlarlas y corregirlas.
- Evaluar y revisar la raíz de la no conformidad con el fin de eliminar las causas de la misma y evitar que se vuelva a presentar. Es importante, que se verifique si existen no conformidades similares en auditorías previas.
- Comparar las no conformidades presentadas con las acciones correctivas tomadas; esto, con el fin de asegurar que no se vuelvan a presentar y evaluar la efectividad de las acciones correctivas aplicadas.
- Evaluar la efectividad de las acciones correctivas tomadas.
- Realizar los cambios en el sistema que sean necesarios.

- Después de cada revisión, se deberá documentar lo encontrado con el fin de generar la evidencia de las acciones y adicionalmente, permitir ajustar los entregables que sean objeto de modificación en el MSPI.

De acuerdo con lo anterior, es evidente que el modelo y su sistema de gestión es cíclico y deberá estar en continua revisión por parte de la Entidad con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

Una vez sean mejoradas las actividades que correspondan, éstas deberán ser incluidas en el plan de comunicaciones de la entidad a fin de que sea conocida por todos los grupos de interés.

6. Responsables

- Alta Dirección y Comité de Gestión y Desempeño: Responsables de la aprobación de los documentos de alto nivel.
- Responsable de la Seguridad Digital, áreas TIC: Coordinar las actividades de implementación y aseguramiento del MSPI.
- Responsable de Control Interno: Coordinar las auditorías internas enmarcadas en la medición y evaluación del MSPI.

7. Referencias

MINTIC. mintic.gov.co. Obtenido de mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Guías y documentos Política Digital MINTIC. https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150511:Controles-de-seguridad-y-privacidad-de-la-informacion

REVISO	APROBÓ
PROFESIONAL UNIVERSITARIO REQUERIMIENTOS TECNOLOGICOS	GERENTE

CONTROL DE CAMBIOS			
FECHA	**DESCRIPCIÓN DEL CAMBIO**	**VERSIÓN**	**MODIFICADO POR**
14/04/2021	Aprobado por Comité Institucional de Gestión y Desempeño	01	Profesional Universitario de Requerimientos Tecnológicos
22/02/2022	Aprobado por Comité Institucional de Gestión y Desempeño	02	Profesional Universitario de Requerimientos Tecnológicos
30/01/2023	Aprobado por Comité Institucional de Gestión y Desempeño	03	Profesional Universitario de Requerimientos Tecnológicos
28/12/2023 29/01/2024	Actualización socializada y viabilizada por Comité Institucional de Gestión y Desempeño No 13/2023 Actualización Aprobada por Comité de Institucional de Gestión y Desempeño No 01/2024.	04	Comité Institucional de Gestión y Desempeño

Reviso Aspectos de Calidad: Lorena Aguirre, Profesional Universitario – Planeación