Firma de Autorizaciones		
Elaboró	**Revisó**	**Aprobó**
Zulay García **Contratista**	**Jefe Oficina Asesora de Planeación**	**Comité Institucional de Gestión y Desempeño**
Control de Cambios		
Fecha	**Descripción**	
Diciembre 2023	Creación del Documento de acuerdo al articles-237872_modelo maestro_mspi MinTIC octubre 2021.	

Contenido

Lista de Tablas

Lista de Ilustraciones

1. INTRODUCCIÓN

En consecuente con la realidad de que las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía[1], el IDEP, adopta los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, en adelante Min TIC, con el objetivo de generar confianza en el uso del entorno digital y el máximo aprovechamiento de las de las tecnologías de la información y las comunicaciones.

Mediante los lineamientos dados por Min TIC para la implementación de la estrategia de seguridad digital, se articula el sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; con el MSPI que de cinco (5) fases, las cuales permiten que la Entidad pueda gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, se abordan las siguientes fases:

Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.

Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

[1] articles-5482_Modelo_de_Seguridad_Privacidad.pdf

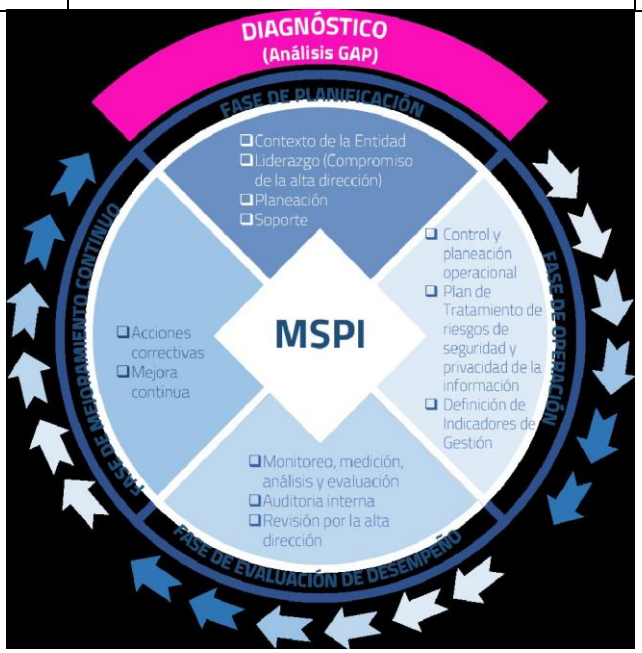

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

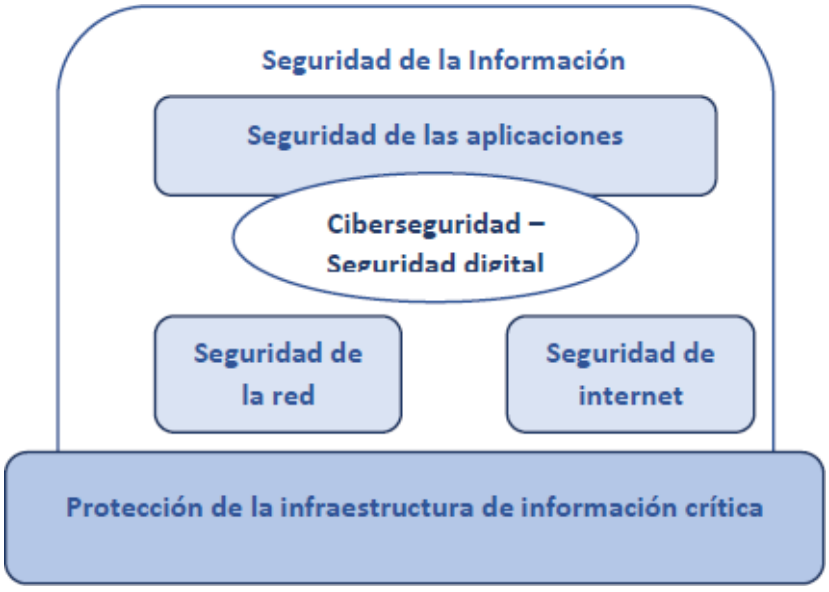

Ilustración 2 Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)

2. AUDICIENCIA

El presente documento está dirigido al talento humano que integra al Instituto para la Investigación Educativa y Desarrollo Pedagógico - IDEP.

3. DEFINICIONES[2]

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

- **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 dicho riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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

[2] Modelo de Seguridad y Privacidad de la Información (MSPI), Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC, febrero 2021)

Tratamiento (Ley 1581 de 2012, art 3)

- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

- **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 literal h)

- **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **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).

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados

del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- **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 a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

4. OBJETIVOS Y ALCANCE[3]

4.1. OBJETIVO GENERAL

Generar un documento de buenas prácticas en Seguridad y Privacidad de la Información del IDEP.

4.2. OBJETIVOS ESPECÍFICOS[4]

- Adoptar, implementar y apropiar el MSPI por medio de los mecanismos, lineamientos e instrumentos de implementación proporcionados por el Min TIC.

- Aportar en el desarrollo e implementación de la estrategia de seguridad digital de la Entidad.

- Establecer procedimientos de seguridad que permitan al Instituto apropiar el habilitador de seguridad en la política de Gobierno Digital.

- Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de la entidad.

- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.

- Contribuir en el desarrollo y ejecución del plan estratégico institucional de la entidad, a través del plan de seguridad y privacidad de la información.

[3] Tomados del Anexo 1 MSPI MinTIC, febrero 2021.

[4] Tomados del Anexo 1 MSPI MinTIC, febrero 2021.

4.3. ALCANCE

Continuar fortaleciendo las políticas de seguridad y privacidad de la información, manteniendo la preservación de la confidencialidad, integridad, disponibilidad de la información y permitiendo garantizar la privacidad de los datos, mediante el desarrollo del plan de seguridad y privacidad de la información y el plan de tratamiento de riesgos de la seguridad y privacidad de la información para la vigencia 2023.

MARCO JURÍDICO[5]

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

[5] nexo 1, Modelo de Seguridad y Privacidad de la información (MSPI), del Ministerio de Tecnologías de la información y Comunicaciones (MinTIC).Febrero 2021.

5. FASE DE DIAGNÓSTICO

Esta fase permite ver el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se realiza un diagnóstico de la Entidad utilizando el "Instrumento de evaluación del MSPI", [6] con el que se identifica de forma específica los controles implementados y faltantes que son insumos fundamentales para la fase de planificación.

A continuación, se muestra las etapas previas a la implementación:

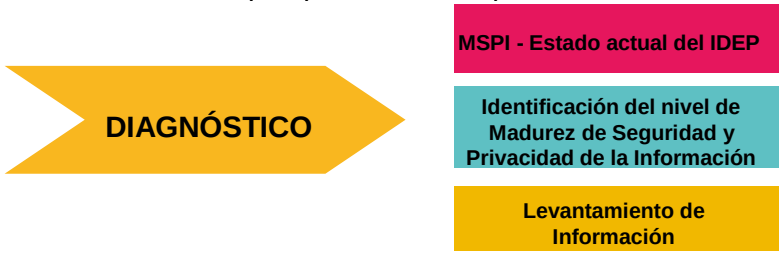

Ilustración 3 Etapas previas a la implementación

5.1. Estado actual del IDEP

Acogiendo las directrices de Gobierno digital, el IDEP estableció una política de seguridad y privacidad de la información que se actualiza según la necesidad y es pública por medio de la web de la entidad, de igual manera acoge la resolución 040 de 2017 por la cual se adopta la política de privacidad y tratamiento de datos personales.

A pesar de que Gobierno Digital evoluciona permanentemente y que de la misma manera para su cumplimiento exige grandes retos incluyendo los recursos necesarios, el IDEP por medio del proceso de Gestión Tecnológica, en lo posible acoge las directrices de la política de gobierno digital, y con los recursos reducidos tanto en talento humano como en presupuesto para la adquisición de tecnología, se gestionan y se llevan a cabo procesos de actualización e implementación en infraestructura tecnológica que ayudan a implementar los controles de seguridad físicos y lógicos que en cierta manera hacen frente a los diferentes riesgos de los que toda entidad está expuesta a sufrir incidentes de seguridad digital. Por otra parte, se realiza actualización y reporte de los instrumentos de seguimiento como son: Plan de seguridad y privacidad de la información, plan de tratamiento de riesgos, plan de mantenimiento y monitoreo, mapa de riesgos y la política de seguridad y privacidad de la información.

[1] articles-150507_Instrumento_Evaluacion_MSPI IDEP 23102023

Por otra parte, el Modelo de Seguridad y Privacidad de la Información (en adelante MSPI), como parte integral de las Políticas de Gobierno digital y Seguridad Digital del MIPG, cuenta como primera etapa con el plan de trabajo con el que se está elaborando la versión inicial del documento MSPI, para lo cual se inició con la actualización de la herramienta de evaluación del MSPI y anexo Diagnostico de Datos Personales-Controles de seguridad (articles-150507, articles-5482 según MinTIC) base fundamental para el desarrollo del documento versión preliminar, sin embargo es necesario tener en cuenta que para llevarlo a cabo en el año 2024 se debe contar con los recursos humanos y tecnológicos necesarios. Teniendo en cuenta que nuestra recomendación es ampliar la auditoría a toda la Entidad para dar una cobertura completa a las acciones a llevar a cabo en cuanto a Gobierno Digital y Seguridad Digital, esto antes de dar inicio al plan mencionado, con el propósito de alcanzar un nivel de madurez simétrico en la Entidad al respecto de estos temas.

Están correctamente incluidos y catalogados los activos de información, en las tres dimensiones de Confidencialidad, Disponibilidad e Integridad, sin embargo, se tiene planeado contemplar todos los dominios dentro del MSPI.

Por medio de la herramienta de autodiagnóstico (Análisis GAP), se identificó el estado actual del IDEP con respecto a la Seguridad y privacidad de la Información, en los aspectos como:

- La línea base de seguridad por medio de la hoja levantamiento de información:
- Datos básicos de la entidad, preguntas
- Datos e información general como base para la evaluación y diagnóstico de la entidad.
- Grupo MSPI – IDEP, áreas involucradas.
- Identificación de La Línea Base De Seguridad Administrativa y Técnica.

Para la calificación de cada uno de los dominios, se hizo uso de la Tabla de escala de valoración de controles que hace parte del Instrumento de evaluación del MSPI:

Tabla de Escala de Valoración de Controles		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 1 Tabla de Escala de Valoración de Controles

5.2. Nivel de madurez modelo seguridad y privacidad de la información

El instrumento de evaluación presenta los siguientes niveles de madurez del modelo seguridad y privacidad de la información:

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	INTERMEDIO
Definido	INTERMEDIO
Administrado	INTERMEDIO
Optimizado	CRÍTICO

Tabla 2 Niveles de cumplimiento

Descripción de los niveles de madurez del modelo seguridad y privacidad de la información:

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Tabla 3 Descripción de niveles de cumplimiento

Calificación de acuerdo al cumplimiento de requisitos:

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Tabla 4 Requisitos con calificaciones de cumplimiento

- **Calificación frente a mejores prácticas en ciberseguridad (NIST)**

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
FUNCION CSF	CALIFICACIÓN ENTIDAD	**NIVEL IDEAL CSF**
DETECTAR	60,00	100
IDENTIFICAR	59,83	100
PROTEGER	53,78	100
RECUPERAR	53,33	100
RESPONDER	47,78	100

Tabla 5 Modelo Framework Ciberseguridad NIST

De acuerdo al Instrumento de evaluación, se refleja la calificación de la entidad en su función CSF dentro del modelo de Ciberseguridad NIST.

5.3. Levantamiento de Información

Dentro del levantamiento de información y de acuerdo a la calificación obtenida por medio de la a aplicación de la tabla de escala de valoración de controles, se identificó el nivel de madurez de seguridad y privacidad de la información en el que se encuentra la entidad, y se tienen los siguientes resultados:

- **Evaluación de efectividad de controles - ISO 27001:2013 Anexo A**

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	63	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	82	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	60	100	EFECTIVO
A.9	CONTROL DE ACCESO	68	100	GESTIONADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	52	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	55	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	47	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	62	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	54	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	57,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		56	100	EFECTIVO

Tabla 6 Evaluación de efectividad de controles

Se identifica que de acuerdo al avance reportado en cada dominio, se tiene una calificación total actual de 56 sobre la calificación objetivo del 100, también la tabla indica la evaluación de efectividad del control por cada dominio.

- **Avance ciclo de funcionamiento del modelo de operación (PHVA)**

Año	AVANCE PHVA		
	COMPONENTE	% de	% Avance Esperado
2023	Planificación	22%	40%
	Implementación	6%	20%
	Evaluación de desempeño	7%	20%
	Mejora continua	8%	20%
TOTAL		43%	100%

Tabla 7 Avance PHVA

Con respecto al modelo de operación PHVA, se refleja el porcentaje de avance para cada uno de sus componentes y el avance total del 43% sobre el avance esperado del 100%.

De otra manera se puede ver el ciclo de funcionamiento del modelo de operación:

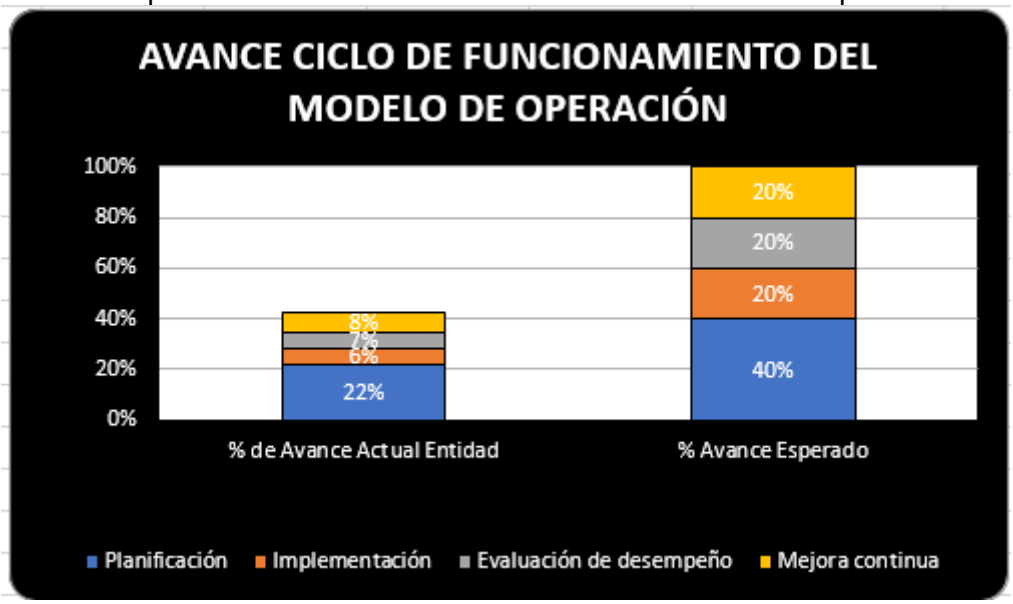

Ilustración 4 Avance ciclo de funcionamiento del modelo de operación

6. FASE 1: PLANIFICACIÓN

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

6.1. CONTEXTO

7.1.1. Comprensión de la organización y su contexto

El Instituto para la Investigación Educativa y el Desarrollo Pedagógico, IDEP, fue creado mediante Acuerdo 26 de 1994, expedido por el Concejo de Bogotá. De conformidad con el artículo 1 y 6 de la norma de creación, el IDEP es un establecimiento público, con personería

jurídica, autonomía administrativa y patrimonio propio, cuya dirección y administración corresponde al Consejo Directivo y al Director Ejecutivo, quien será su representante legal. Igualmente, el literal d) del artículo 8 del Acuerdo 26 de 1994 es función del Consejo Directivo determinar la estructura administrativa del Instituto y la planta de personal. La Resolución 04 de 2007, definió la estructura.

Misión

Fortalecer y gestionar la investigación y la innovación, así como el desarrollo pedagógico y profesional docente, con miras a producir conocimiento que aporte al cierre de las brechas socioeducativas, a la garantía del derecho a la educación, a la transformación pedagógica y al reconocimiento del saber docente, para aportar en la construcción de un nuevo contrato social y ambiental.

Visión

En 2030, el IDEP será reconocido a nivel distrital, nacional e internacional como un centro de investigación, innovación y desarrollo pedagógico de la más alta calidad académica que produce conocimiento relevante, pertinente y riguroso orientado a la transformación educativa y pedagógica, al desarrollo profesional docente y a la garantía del derecho a la educación.

Objetivos Estratégicos

Fortalecer la apropiación, uso y divulgación del conocimiento producido por el IDEP, de los y las maestras, como aporte al cierre de las brechas de la calidad educativa, a la transformación pedagógica y al reconocimiento del saber docente.

Objetivos Específicos:

1. Producir investigaciones en el IDEP, para contribuir al cumplimiento de las metas sectoriales de cierre de brechas y de transformación pedagógica en el marco del ODS 4.
2. Optimizar la gestión de la información y el conocimiento producido a través de los procesos de seguimiento a la política sectorial para su uso y apropiación por parte de los grupos de interés.
3. Aumentar el nivel de transferencia del conocimiento producido por el IDEP al campo educativo y del sector.
4. Implementar una estrategia articulada de promoción y apoyo a colectivos, redes, y docentes investigadores e innovadores de los colegios públicos de Bogotá.
5. Implementar una estrategia de desarrollo pedagógico permanente y situada, para la investigación, la innovación y la sistematización de las prácticas con enfoque territorial.
6. Implementar una estrategia efectiva de socialización, divulgación y gestión del conocimiento derivado de las investigaciones y publicaciones del IDEP y de los docentes del Distrito.
7. Implementar una estrategia para el fortalecimiento institucional.

Acto administrativo del 25 de enero de 2021, Acta N° 2 del Comité Institucional de Gestión y Desempeño del IDEP.

7.1.2. Necesidades y expectativas de los interesados

El Instituto no cuenta con la existencia de una oficina o área de TI. Por medio del procedimiento "Gestión Tecnológica" que hace perta de la Oficina Asesora de Planeación (OAP), se espera cumplir con los lineamientos de TI como dispone Gobierno Digital.

7.1.3. Definición del alcance del MSPI

La seguridad y privacidad de la información es transversal a todas las oficinas y subdirecciones del Instituto, de igual forma permea los objetivos misionales, procesos, servicios y sistemas de información.

6.2. LIDERAZGO

7.2.1. Liderazgo y compromiso

El IDEP cuenta con el comité Institucional de Gestión y desempeño, fue creado por la Resolución 024 de 2019 "*por la cual se crea y establece el reglamento de funcionamiento del Comité Institucional de Gestión y desempeño del Instituto para la Investigación Educativa y el Desarrollo Pedagógico, IDEP*".

De acuerdo con lo establecido en el Artículo 4, el comité Institucional de Gestión y Desempeño se encuentra integrado así:

- El (la) directora(a) General (quien lo presidirá)
- El (la) subdirector(a) Administrativo(a) y Financiero(o)
- El (la) subdirector(a) Académico(a)
- El (la) jefe de la oficina Asesora de planeación (quien ejerce la Secretaría Técnica)
- El (la) jefe de la Oficina Jurídica
- El (la) jefe de la Oficina de Control Interno (invitado permanente con voz, pero sin voto)

Mediante la resolución 133 de 2020 se actualizó el reglamento de su funcionamiento.

7.2.2. Política de Seguridad y Privacidad de la Información

La política de seguridad y privacidad de la información es actualizada cada vez que se requiere de acuerdo a revisiones internas y de acorde a lo exigido por Gobierno Digital.
La política está aprobada y publicada en el portal web institucional así:
PO-GT-12-01 Política Seguridad y privacidad de la información

7.2.3. Roles y responsabilidades

El Instituto para la Investigación Educativa y el Desarrollo Pedagógico, IDEP, fue creado mediante Acuerdo 26 de 1994, expedido por el Concejo de Bogotá. De conformidad con el artículo 1 y 6 de la norma de creación, el IDEP es un Establecimiento Público, con personería jurídica, autonomía administrativa y patrimonio propio, cuya dirección y administración corresponde al Consejo Directivo y al Director Ejecutivo, quien será su representante legal. Igualmente, el literal d) del artículo 8 del Acuerdo 26 de 1994 es función del Consejo Directivo determinar la estructura administrativa del Instituto y la planta de personal.

De conformidad con la Resolución 09 de 2002, expedida por el Consejo Directivo del IDEP, la estructura organizacional del Instituto es la siguiente:

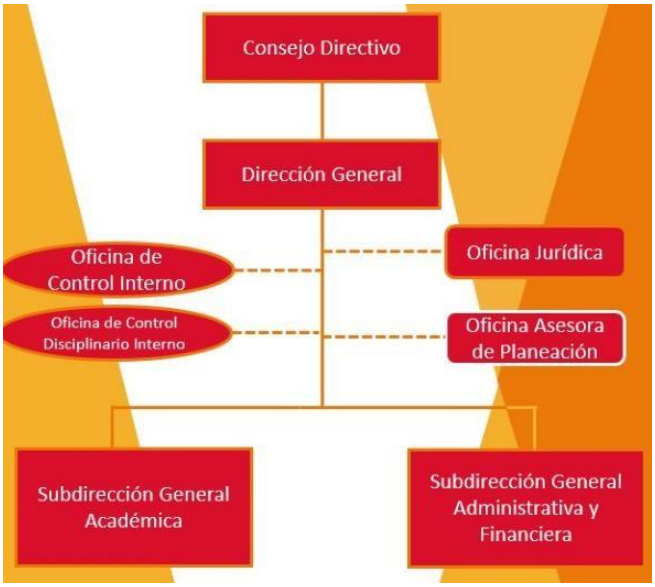

Ilustración 8 Estructura organizacional IDEP

Según la resolución 009 de 2022, “Por medio de la cual se modifica la planta de empleos del Instituto para la Investigación Educativa y el Desarrollo Pedagógico”, queda de la siguiente manera de acuerdo a los artículos segundo y tercero:
ARTÍCULO SEGUNDO: Crear en la planta de empleos del Instituto para la Investigación Educativa y el Desarrollo Pedagógico – IDEP – los siguientes empleos:

Tabla 8 Planta de empleos IDEP

DENOMINACIÓN DEL EMPLEO	CÓDIGO	GRADO	NÚMERO DE CARGOS
Director General de Entidad Descentralizada	050	05	Uno (1)
Subdirector General de Entidad Descentralizada	084	04	Dos (2)
Jefe de Oficina	006	03	Uno (1)
Jefe de Oficina	006	02	Uno (1)
Jefe de Oficina	006	01	Uno (1)
Total número de empleos creados			Seis (6)

ARTÍCULO TERCERO: Las funciones propias del Instituto para la Investigación Educativa y el Desarrollo Pedagógico – IDEP, serán cumplidas por la planta de empleos que a continuación se señala:

DENOMINACIÓN DEL EMPLEO	CÓDIGO	GRADO	No. DE EMPLEOS
DESPACHO DEL DIRECTOR			
Director General de Entidad Descentralizada	050	05	Uno (1)
Asesor	105	03	Uno (1)
Asesor	105	02	Dos (2)
Secretario Ejecutivo	425	05	Uno (1)
Conductor	480	03	Uno (1)
PLANTA GLOBAL			
Subdirector General de Entidad Descentralizada	084	04	Dos (2)
Jefe de Oficina	006	03	Uno (1)
Jefe de Oficina	006	02	Uno (1)
Jefe de Oficina	006	01	Uno (1)
Jefe de Oficina Asesora de Planeación	115	01	Uno (1)
Profesional Especializado	222	07	Dos (2)
Profesional Especializado	222	06	Uno (1)
Profesional Especializado	222	05	Dos (2)
Tesorero General	201	04	Uno (1)
Profesional Especializado	222	04	Uno (1)
Profesional Especializado	222	03	Cuatro (4)
Profesional Universitario	219	02	Uno (1)
Profesional Universitario	219	01	Dos (2)
Técnico Operativo	314	02	Uno (1)
Técnico Operativo	314	01	Tres (3)
Secretario Ejecutivo	425	05	Tres (3)
Secretario Ejecutivo	425	04	Dos (2)
Auxiliar Administrativo	407	02	Uno (1)
Operario	487	01	Dos (2)
TOTAL PLANTA DE EMPLEOS	**TREINTA Y OCHO (38)**		

Tabla 29 Planta de empleos IDEP 2

De acuerdo a la normatividad actual, su propósito es:

- **DIRECCIÓN GENERAL**. Según la resolución 161 de 2022. Formular las políticas institucionales en coordinación con el Consejo directivo y definir, adoptar y dirigir los

planes, programas y proyectos que deben ejecutar las dependencias de la entidad para lograr el cumplimiento de la misión y los objetivos institucionales.

- **OFICINA ASESORA DE CONTROL INTERNO**. Según la resolución 161 de 2022. Verificar y evaluar el estado del sistema de control interno, de acuerdo con la normatividad vigente.
- **OFICINA ASESORA JURÍDICA**. Según la resolución 161 de 2022. Dirigir los asuntos jurídicos, la gestión contractual y de defensa judicial del Instituto de acuerdo con la normatividad vigente y llevar a cabo la etapa de juzgamiento dentro del proceso disciplinario interno, de conformidad con lo establecido en la normatividad vigente y contribuyendo a la prevención del daño antijurídico.
- **OFICINA DE CONTROL DISCIPLINARIO INTERNO**: Según la resolución 161 de 2022. Adelantar la etapa de instrucción en primera instancia de los procesos disciplinarios que se adelanten en contra de los servidores y ex servidores públicos, en los términos de oportunidad, de conformidad con la normatividad vigente sobre la materia.
- **OFICINA ASESORA DE PLANEACION**. Según la resolución 009 de 2021. Asistir técnica y administrativamente los diferentes niveles en la toma de decisiones de acuerdo con la naturaleza del cargo para que se logre el cumplimiento de los objetivos institucionales.
- **SUBDIRECCIÓN GENERAL ADMINISTRATIVA y FINANCIERA**. Según la resolución 161 de 2022. Dirigir los procesos administrativos, financieros y de recursos humanos del Instituto, de acuerdo con los lineamientos que apoyen el cumplimiento de los objetivos misionales del IDEP.
- **SUBDIRECCIÓN GENERAL ACADÉMICA**. Según la resolución 161 de 2022. Formular, coordinar y dirigir los planes, programas, proyectos e investigaciones, vinculando referentes de la comunidad académica del distrito Capital en su gestión, a través de los cuales el IDEP cumpla con los objetivos misionales.

Normativamente el IDEP no cuenta con una estructura organizacional para las TI. Dentro del manual de funciones se cuenta con el siguiente talento humano:

1 Jefe Oficina Asesora de Planeación, función No. 9: Asesorar a la Dirección General en el manejo de las relaciones interinstitucionales de cooperación con organismos del orden distrital, nacional e internacionales en materia de Ciencia Tecnología e Innovación.
1 Técnico operativo, cuyo objeto es: Apoyar, administrar, controlar y evaluar el desarrollo de los procesos y procedimientos que se requieran y estén relacionados con los sistemas de información del Instituto.

Con lo anterior, la estructura y organización humana TI, está conformada por:

- Un líder de proceso en cabeza de la jefe de la Oficina Asesora de Planeación,
- Un técnico operativo

- Tres profesionales contratistas, quienes atienden las necesidades tecnológicas del instituto.
- Una auxiliar administrativa asistiendo operativamente actividades de gestión administrativa.

6.3. PLANIFICACIÓN

7.3.1. Identificación de activos de información e infraestructura crítica

El Instituto tiene determinados e identificados los activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.

Se tiene clasificados los activos de información de acuerdo a los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.

Se cuenta con el Inventario de activos de información tipo software, hardware y servicios 2020 publicado. Ultima vez que se actualizó 2022. Se señala el criterio de importancia del activo y el responsable del activo.

Se cuenta con el procedimiento PRO-GT-12-07 Registro de Activos de Información software, hardware y servicio del IDEP.

Para el uso aceptable de los activos e cuenta con las siguientes herramientas:
MN-GT-12-15 Manual para la Gestión de los Sistemas de Información del IDEP FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del IDEP PO-GT-12-01 Política Seguridad y privacidad de la información.

Para la devolución de activos se cuenta con:
FT-GC-08-10 Estudios y documentos previos modalidad de contratación directa jurídico o natural. Item 9 obligaciones generales del contratista.
PRO-GTH-13-08 Vinculación de Servidores
PRO-GTH-13-11 Desvinculación de Servidores Suscripción del acuerdo de confidencialidad
FT-GTH-13-21 Acta de entrega e cargo por retiro del servicio

7.3.2. Valoración de los riesgos de seguridad de la información

Cierta valoración de los riesgos de seguridad de la información se encuentra dentro del plan de tratamiento de riesgos de seguridad, pero aún no se tiene un procedimiento procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno.

7.3.3. Plan de tratamiento de los riesgos de seguridad de la información

Se cuenta con el plan de tratamiento de riesgos de seguridad de la información, el cual es actualizado trimestralmente. Este plan se publica en el portal web del Instituto, formalizado así: PL-GT-12-05 Plan Tratamiento riesgos de seguridad y privacidad de la información 2023.

6.4. SOPORTE

7.4.1. Recursos

De acuerdo a los recursos del Instituto y a las necesidades más importantes, la entidad determina y proporciona los recursos financieros y humanos para las acciones a desarrollar y que hacen parte del MSPI. Los recursos se proyectan en el Plan Anual de Adquisiciones el cual también es publicado en el portal web.

7.4.2. Competencia, toma de conciencia y comunicación

Se fortaleció el acceso a las TIC con las condiciones y medios de acercamiento a las mismas y a los diferentes grupos de Interés para la Infraestructura, servicios, aplicaciones, políticas y programas.

Se realiza Alfabetización Digital, mediante el proceso de formación de competencias básicas para el uso de las TIC. Se realiza capacitación por demanda de las diferentes aplicaciones y sistemas de información que se usan en el IDEP, Políticas de seguridad, seguridad digital, uso responsable y destrezas digitales de los usuarios para con las redes sociales y la institucional.

Se dispone de dos repositorios en nube que contienen la información relevante de los sistemas de información crítico7s (Humano - Liquidador de Nómina y Goobi: Administrativo y Financiero) con videos de sesiones de trabajo conjunto donde se resuelven casos puntuales, manuales e instructivos que permiten el uso de los sistemas.

En cuanto a la Ciberseguridad, se implementó y fortaleció el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, formación, prácticas idóneas, seguros y tecnologías que se implementaron buscando la disponibilidad, integridad, autenticidad, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Metas, Resultados e Instrumentos de la Fase de Planificación

Planificación			
Metas	**Resultados**	**INSTRUMENTOS MSPI**	**MRAE**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad y publicada en la web. PO-GT-12-01 Política Seguridad y privacidad de la información	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08
Políticas de seguridad y privacidad de la información	MN-AC-10-02 Manual interno de políticas y procedimientos de protección de datos personales PO-AC-10-02 Política de privacidad y tratamiento de datos personales	Guía no 2 - Política General MSPI	LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	LI.GO.07 LI.GO.08 LI.GO.09
Roles y responsabilidades de seguridad y privacidad de la información.	Comité Institucional de Gestión y desempeño fue creado por la Resolución 024 de 2019. Comité asesor de ciencia, tecnología e innovación, se conformó mediante la Resolución 107 de 2020	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09
Inventario de activos de información.	FT-GT-12-19 Inventario activos de información Tipo Software, Hardware y Servicios IDEP Identificación, valoración y clasificación de activos de información por Oficinas y Subdirecciones.	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23

Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental	LI.SIS.01 LI.ST.05
Identificación, Valoración y tratamiento de riesgo.	PL-GT-12-05 Plan Tratamiento riesgos de seguridad y privacidad de la información 2023 Matriz de riesgos	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad	LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14
Plan de Comunicaciones.	PRO-GTH-13-06 Gestión de Capacitaciones PL-GTH-13-01 Plan Institucional de Capacitación Vigencia 2023	Guía No 14 - Plan de comunicación, sensibilización y capacitación	LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	

Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14 LI.INF.04
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

A continuación, se explica de manera general la fase de planificación del Modelo de Seguridad y Privacidad de la Información.

Política de Seguridad y Privacidad de la Información

La Dirección General del IDEP, entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación de prácticas orientadas a preservar la protección de los activos de información de la Entidad con el fin de minimizar los riesgos por pérdida de confidencialidad, disponibilidad o integridad de la información.

Implementación de la política de Seguridad y Privacidad de la Información

Para la implementación de la presente política de Seguridad y Privacidad de la Información, el IDEP cuenta con los siguientes instrumentos que están disponibles en el sitio web del Instituto:

- **Proceso gestión tecnológica:** El objetivo de este proceso es proveer y mantener los recursos de Tecnología de Información y Comunicación necesarios para el funcionamiento del IDEP.
- **PRO-GT-12-05 Procedimiento para el mantenimiento de infraestructura tecnológica:** Este procedimiento indica la forma como el IDEP realiza el mantenimiento de su infraestructura tecnológica y mantiene actualizada la base de datos de los activos de información de información tipo software, hardware y servicios.
- **PRO-GT-12-07 Procedimiento registro de activos de información tipo software, hardware y servicios:** Este procedimiento inicia con la identificación e ingreso de información de los activos de información y termina con la actualización de la información de los activos de información, así como la generación de los informes respectivos.
- **PRO-GT-12-08 Procedimiento formulación y seguimiento al PETIC:** El objetivo de este procedimiento es mantener actualizado el PETIC, el cual está dirigido al soporte de los objetivos, planes y estrategias del IDEP en tecnologías de información y comunicación TICs, permitiendo dar continuidad al proceso de actualización y modernización de la gestión.
- **PRO-GT-12-10 Procedimiento mesa de servicios:** El objetivo de este procedimiento es registrar y gestionar las solicitudes de soporte técnico a usuarios y de la infraestructura y servicios de tecnología.
- **IN-GT-12-01 Instructivo para la asignación de usuarios**: Este documento establece los parámetros para la creación de cuenta de usuario en los diferentes medios de

procesamiento de información y finaliza con la desactivación de las mismas al momento de desvinculación del funcionario o contratista del Instituto.

- **FT-GT-12-16 Formato para el control de BackUps y revisión de servidores:** Este documento establece los parámetros para el control de BackUps y revisión de servidores del IDEP.

- **PL-GT-12-01 Plan estratégico de tecnologías de la información y comunicaciones PETIC:** Este documento presenta el contexto general de las tecnologías de la información y comunicaciones al interior del IDEP, identificar las necesidades tecnológicas, identifica las herramientas que permiten el aprovechamiento de los recursos tecnológicos y de inversión, describe las estrategias y proyectos que se ejecutarán en el IDEP en la vigencia, en cumplimiento de sus funciones misionales y de visión propuestos en el Plan Estratégico Institucional.

- **PL-GT-12-02 Plan de Contingencia Tecnológica IDEP:** Este documento presenta el plan que permite garantizar el funcionamiento de la tecnología informática y la recuperación en el menor tiempo posible ante una falla que interrumpa la prestación de los servicios alterando la correcta operación de la entidad.

- **FT-GT-12-19 Inventario de activos de información tipo software, hardware y servicios:** Es una base de datos de los activos de información tipo software, hardware y servicios; este documento se actualiza una vez al año.

- **Diagrama de Infraestructura Tecnológica:** Este documento es un diagrama básico de la infraestructura informática del hardware del IDEP.

- **PO-GT-12-01 Política de privacidad y tratamiento de datos:** Este documento establece las políticas en seguridad de la información, para la debida protección de los derechos de los usuarios, visitantes, ciudadanos y demás personas que suministran sus datos personales al IDEP por los diferentes canales de atención y medios de recolección de información. La política fue adoptada mediante Resolución No. 040 de 2017.

- **Manual interno de políticas y procedimientos de protección de datos personales:** El objetivo de este documento es garantizar el adecuado cumplimiento de la Ley 1581 de 2012 y en especial, la atención de consultas y reclamos. Asimismo, dar cumplimiento al Artículo 13 del Decreto 1377 de 2013, en el cual se establece la obligatoriedad por parte de los responsables del tratamiento de datos, de desarrollar sus políticas para el manejo de los datos personales y velar porque los encargados del tratamiento den cabal cumplimiento a las mismas y al Decreto 886 de 2014, que regula lo relacionado al Registro Nacional de Bases de Datos.

- **PL-GT-12-04 Plan seguridad de la información:** Este documento contiene las actividades que el IDEP se compromete a ejecutar en la vigencia, en lo que corresponde

a políticas de seguridad de la información, organización de la seguridad de la información, gestión de activos y control de acceso.

- **PL-GT-12-05 Plan tratamiento de riesgos de seguridad de la información:** Este documento contiene las actividades que el IDEP se compromete a ejecutar en la vigencia, en lo que corresponde al tratamiento de riesgos de seguridad de información de acuerdo con el Modelo de seguridad y privacidad de la información.
- **FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del IDEP:** Este documento los funcionarios y contratistas evidencian mediante su firma su compromiso con el cumplimiento de las normas definidas por el IDEP para minimizar los riesgos de seguridad de la información y optimizar el uso de los recursos tecnológicos del Instituto.

Plan de revisión y seguimiento a la implementación del MSPI.

En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

- ✓ Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- ✓ Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- ✓ Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- ✓ Seguimiento al alcance y a la implementación del MSPI.
- ✓ Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- ✓ Medición de los indicadores de gestión del MSPI
- ✓ Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

8. FASE 2: OPERACIÓN

8.1. Planificación e Implementación

El Instituto realiza la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, y se lleva carpeta de evidencias. Los documentos son revisados, aprobados y publicados en el portal web.

PL-GT-12-05 Plan Tratamiento riesgos de seguridad y privacidad de la información 2023.

Por otra parte se tienen implementados los siguientes controles:

Para la política de control de acceso, se usan los siguientes instrumentos:

- PO-GT-12-01 Política Seguridad y privacidad de la información
- Política de Privacidad y Tratamiento de Datos - Resolución 40 de 2017
- FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del IDEP
- IN-GT-12-01 Instructivo para la asignación de usuarios
- IN-GT-12-05 - Instructivo para cambio de contraseña de ingreso a los sistemas de información del IDEP.
- MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS
- PERSONALES

Para el acceso a redes y a servicios en red:
Se tiene el MN-GT-12-07 Manual para la administración de la red LAN del IDEP y políticas de seguridad

Para la gestión de acceso a usuarios y responsabilidad de usuarios, se tienen los siguientes instrumentos:

- IN-GT-12-01 Instructivo para la asignación de usuarios IN-GT-12-05 - Instructivo para cambio de contraseña de ingreso a los sistemas de información del IDEP FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del IDEP
- MN-GT-12-12 Manual para la administración de los sistemas de información
- FT-GTH-13-46 Formato Acuerdo de confidencialidad de funcionario o servidor público

Para el control de acceso a los sistemas de información:

- PO-GT-12-01 Política Seguridad y privacidad de la información
- Se tienen controles a través del directorio activo. Uso de reglas por directorio activo.
- Se tiene control de acceso al data center a través de biométrico.
- PO-GT-12-01 Política Seguridad y privacidad de la información.
- Las contraseñas temporales se entregan personalmente.
- Se realiza a través de permisos de usuarios en el directorio activo.
- Se tiene un registro de los programas mínimos que tienen los computadores.

9. FASE 3: EVALUACIÓN DE DESEMPEÑO

9.1. Seguimiento, medición, análisis y evaluación.

Se cuenta con varias aristas de seguimiento, medición, análisis y evaluación para el proceso de Gestión Tecnológica, proceso que lidera el MSPI, dentro de los cuales, se tiene el reporte que se hace a la Alta consejería con el diligenciamiento del instrumento de evaluación MSPI, diligenciamiento del FURAG, que contiene el aparte de Seguridad Digital, internamente el Instituto realiza auditoría interna, del cual se tiene el plan de mejoramiento.

El plan de mejoramiento y los informes de auditoría se encuentran publicados en el portal web del Instituto.

Igualmente, se hace el reporte trimestral de los avances en el plan de acción, plan de tratamiento de riesgos, hoja de vida del indicador de seguridad y privacidad de la información

9.2. Auditoría interna

La oficina de control interno realiza anualmente la programación y ejecución de la auditoría interna al proceso de gestión tecnológica, del cual emite un informe, al cual se le da respuesta y posteriormente publica en el portal web del Instituto.

9.3. Revisión por la dirección

Revisar el MSPI de la entidad, por parte de la alta dirección (comité de gestión institucional), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

De la revisión a la implementación, se requieren los siguientes documentos:
• Acta y documento de Revisión por la Dirección.
• Compromisos de la Revisión por la Dirección.

10. FASE 4: MEJORAMIENTO CONTÍNUO

10.1. Mejora

Es importante que la entidad elabore un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI, con el propósito de identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

ANEXOS

1. articles-150507_Instrumento_Evaluacion_MSPI IDEP 23102023

2. PL-GT-12-04 Plan Seguridad y Privacidad de la Información 2023