INSTITUTO DEPARTAMENTAL DEL DEPORTE, LA EDUCACIÓN FÍSICA, LA RECREACIÓN Y APROVECHAMIENTO DEL TIEMPO LIBRE DEL HUILA - INDERHUILA

Enero de 2023

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Proceso: COMUNICACIONES ESTRATÉGICAS Y TIC

INDERHUILA

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temático de la Estrategia en **seguridad y privacidad de la información**, el cual busca proteger los datos de los ciudadanos garantizando la seguridad de la información.

1. CONTEXTO ESTRATÉGICO INSTITUCIONAL

Nombre del proceso		**COMUNICACIONES ESTRATÈGICAS Y TIC**
Objetivo del proceso		GESTIONAR LAS TECNOLOGÌAS DE INFORMACIÒN Y COMUNICACIONES DEL INDERHUILA, SALVAGUARDANDO LA INFORMACIÒN DE LOS PROCESOS, DESARROLLANDO PLANES, PROGRAMAS Y PROYECTOS, CON UN ADECUADO SOPORTE ADMINISTRATIVO PARA EL BUEN MANTENIMIENTO DE LOS SERVICIOS Y LA INFRAESTRUCTURA TECNOLÒGICA DE LA ENTIDAD.
Alcance del proceso		El proceso inicia con la formulaciòn y/o actualizaciòn de los lineamientos, polìticas de tecnologìas de informaciòn y comunicaciòn e identificaciòn de las necesidades tecnològicas para la informaciòn, divulgaciòn y promociòn de las diferentes planes, programas y proyectos institucionales; y culmina con la ejecuciòn de las estrategias, la entrega de servicios TIC'S y las acciones de uso y aprovechamiento de la informaciòn y comunicaciones.
Para administrar los riesgos de gestión, corrupción y de seguridad digital, se debe analizar el contexto particular al que se enfrentan los procesos ante los 3 tipos de riesgos (de gestión, corrupción y seguridad digital), conforme a la misionalidad; para ello, es necesario definir los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9), estableciendo el contexto interno y externo de la entidad, además del contexto del proceso y sus activos de seguridad digital.		
Contexto Interno	Debilidades	Falta de talento humano para las responsabilidades del proceso y el tamaño de la entidad
		Falta de inversiòn en la infraestructura (servicios especializados, sistema de informaciòn robusto y de equipos tecnològicos y suministros)
		Instalaciones indecuadas para la infraestructura de las telecomunicaciones.
		Falta de colaboraciòn y oportunidad entre las àreas, cuando se requiere informaciòn acerca de temas de su competencia
		Falta de cultura organizacional para visitar la pàgina web del Instituto.
	Fortalezas	Profesional de Sistemas con conocimiento de los procesos de la entidad y sus necesidades
		Profesional de las comunicaciones con conocimiento e idoneidad.
		Procesos documentados en el Sistema Integrado de Gestiòn
		Compromiso del personal asignado al proceso
		Retroalimentaciòn entre la Direcciòn y el personal contratado
Contexto Externo	Oportunidades	Adopciòn e implementaciòn de buenas pràcticas TIC'S a partir de las expeiencias de otras entidades
		Legislaciòn y lineamientos de orden nacional para el fortalecimiento de la gestiòn TIC'S en entidades territoriales
		Visitas a entidades diferentes para conocer mejores pràcticas
	Amenazas	Sanciones por no contar con software licenciado
		No cumplimiento a la normatividad establecida a nivel nacional
		Interrupciòn de las actividades de procesos por la falta de transferencia de informaciòn
		Resistencia al cambio

Contexto del proceso	Diseño del proceso	Claridad en el diseño y alcance descrito en el proceso
	Interacción con otros procesos	Proveedor de servicios TIC'S para los demas procesos de la entidad
	Transversalidad	Con todos los procesos de la entidad
	Procedimientos asociados	Pertinencia con todos los procedimientos y documentos asociados al proceso
	Responsable	Dueño de proceso y profesional especializado asignado
	Comunicación entre los procesos	La comunicaciòn es oportuna entre los procesos
	Activos de seguridad digital del proceso	Ausencia de activos de seguridad digital
	Indicador	
	Meta	Al no lograr determinar la oportunidad en la atenciòn de los requerimientos de asesoria, soporte y mantenimiento en la operaciòn y uso de los servicios tecnològicos y de las comunicaciones del Inderhuila
	Plazo	El incumplimiento de los plazos establecidos para la atenciòn de los requerimientos de asosoria, soporte y mantenimiento en la operaciòn y uso de los servicios tecnològicos y de las comunicaciones del Inderhuila e implementaciòn de las acciones de mejora continua en los procesos
De acuerdo al estudio y análisis anterior, identifique:		
Factores claves de éxito en el proceso		Oportunidad en la prestaciòn del servicio
		Seguridad de la informaciòn (confidencialidad, integridad y disponibilidad)
		Aprobaciòn de los lineamientos impartidos por TIC'S
		Profesional idòneo para la prestaciòn del servicio
Oportunidades que tiene el proceso ¿Qué podría potencializar el cumplimiento del objetivo, meta y plazo asociado al proceso?		Legislaciòn y lineamientos de orden nacional para el fortalecimiento de la gestiòn TIC'S en entidades territoriales
		Adopciòn e implementaciòn de buenas pràcticas TIC'S a partir de las expeiencias de otras entidades
		Procesos documentados en el Sistema Integrado de Gestiòn

1.1 Misión

El INDERHUILA, tiene como misión generar y brindar a la comunidad oportunidades de participación en los procesos de iniciación, formación, fomento y práctica del deporte, la educación física, la recreación y el aprovechamiento del tiempo libre como contribución al desarrollo integral del individuo, apoyando la construcción y adecuación de escenarios deportivos y recreativos para el mejoramiento de la calidad de vida de los Huilenses.

1.2 Visión

El INDERHUILA, con VISION orientada hacia el año 2025, será un Ente Deportivo líder a nivel nacional con innovación y aplicación de ciencia y tecnología en los procesos contribuyendo a la formación de Huilenses más sanos, activos y competitivos.

1.3 Objetivos institucionales (Alineados al Plan)

INDERHUILA tiene por objeto, adoptar para el Departamento las políticas, planes y programas que, en materia de deporte, educación Física, recreación y aprovechamiento del tiempo libre, emite el MINISTERIO DEL DEPORTE, el Gobierno Nacional y el Departamento. En cumplimiento de este objeto promoverá:

1. La práctica del deporte, la educación física, la recreación y el aprovechamiento del tiempo libre como medio para mejorar la calidad de vida de los Huilenses.

2. Generar condiciones para la formación integral de los deportistas.

3. Promover y desarrollar programas y proyectos a través de organizaciones deportivas, recreativas, civiles, educativas y culturales.

2. DESARROLLO ESTRATEGIAS GOBIERNO DIGITAL

2.1 Marco legal

NORMA	DESCRIPCIÓN
Decreto 103 del 20 de enero de 2015	“Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”. “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Decreto 1078 del 26 de mayo de 2015	"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones." 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 2573 de 12 de diciembre de 2014	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Ley 1712 de 2014	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 1499 del 11 de septiembre de 2017	Define los criterios de evaluación y seguimiento de las políticas de gestión y desempeño institucional, buscando la simplificación y racionalización de reportes de información y requerimientos para su implementación y operación
Decreto 612 del 04 de abril 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 1008 del 14 de junio 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 Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

2.2 Alcance

El Plan de Tratamiento de Riesgos de Seguridad Digital presentara los controles y tratamientos definidos para aplicar sobre las causas de los riesgos inherentes de seguridad digital analizados y evaluados para 13 procesos de gestión de la INDERHUILA, producto de la aplicación de la Política Institucional de Gestión de Riesgo, la cual abarca para los riesgos de seguridad digital, el diagnóstico de los activos de seguridad digital de cada uno de los procesos de gestión de la entidad, el nivel de criticidad de los mismos en base a la confidencialidad, integridad y disponibilidad de dichos activos, el análisis de los riesgos de seguridad existentes en base a causas, probabilidad de ocurrencia, nivel de impacto, vulnerabilidades, amenazas relacionadas, y por último la identificación de brechas y no conformidades.

2.3 Objetivos

Mitigar los riesgos asociados a los procesos existentes en el Inderhuila, con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

Específicos:

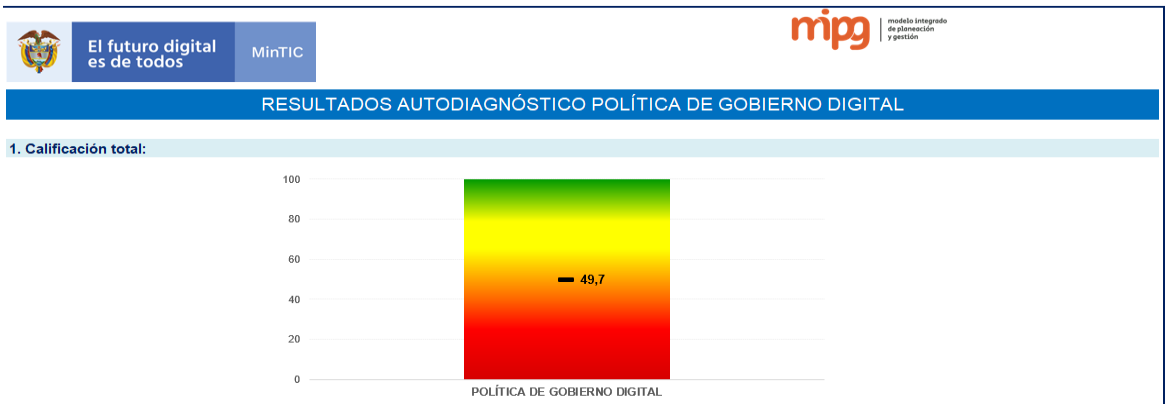
- Implementar las Políticas de la seguridad de la información

- Desarrollar un plan de trabajo para la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información.

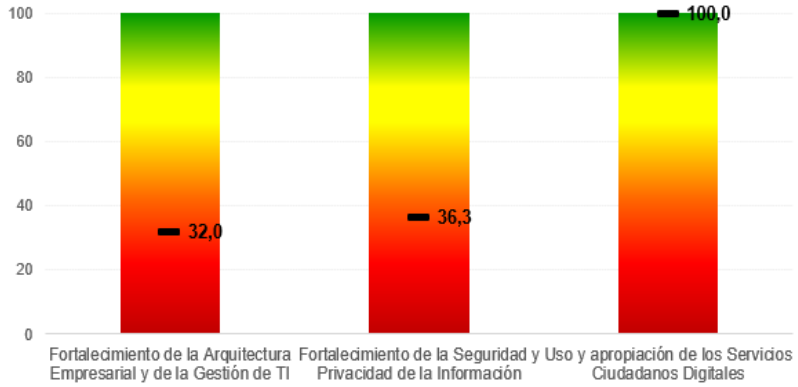
- Aplicar las metodologías del DAPF respectivamente en seguridad y riesgo de la información.

2.4 Diagnóstico de la Política Gobierno Digital

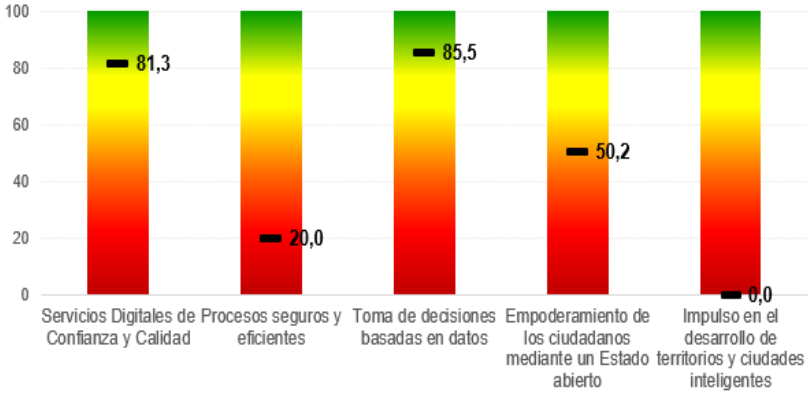
Una vez realizados el autodiagnóstico para la Política Gobierno Digital, que se representa en la siguiente gráfica con un parámetro de calificación de cero (0) a cien (100) puntos, diagnóstico que obtuvo un resultado de 49.7; en el cual se evaluó los habilitadores, fortalecimiento de la arquitectura empresarial y de la gestión TI, fortalecimiento de la seguridad y privacidad de la información y uso y apropiación de los servicios ciudadanos digitales.



2. Calificación de los habilitadores de la Política de Gobierno Digital:



3. Calificación de los propósitos de la Política de Gobierno Digital:



Por lo anterior, resulta imperiosa implementar estrategias para el plan de tratamiento de riesgo de seguridad y privacidad de la información, para dar lugar al fortalecimiento de la seguridad y privacidad de la información, fortalecimiento de la arquitectura empresarial y de la gestión de TI y apropiación de los servicios ciudadanos digitales, con el objetivo de garantizar la accesibilidad y disponibilidad de la información pública a todos los usuarios y partes interesadas, su comprensión y salvaguarda en la protección de datos personales y aumentar la puntuación en general, especialmente en aquellos habilitadores que obtuvieron una puntuación critica, que no le permitirán a la entidad desarrollar un ejercicio de valoración positiva a la dimensión que estructura el Modelo Integrado de Gestión y Planeación MIPG.

2.5 Resultados medición formulario único reporte de avances de la gestión – FURAG

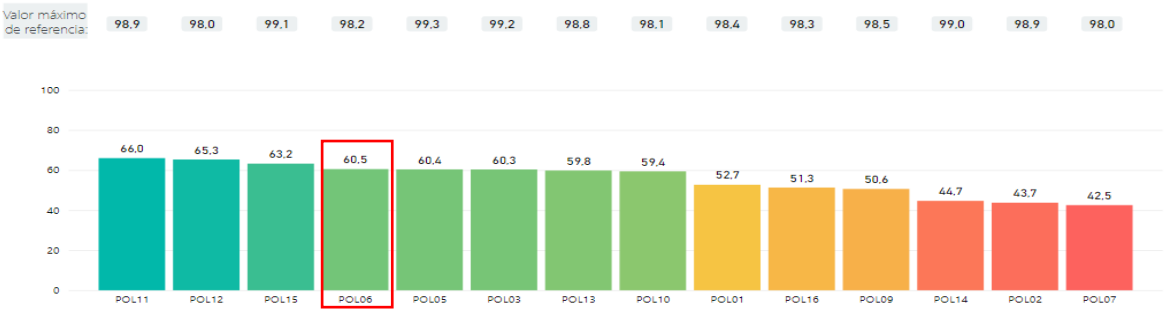
II. Índices de las dimensiones de gestión y desempeño

Dimensión	Puntaje consultado	Valor máximo de referencia
D1: Talento Humano	49,2	98,4
D2: Direccionamiento y Planeación	60,3	99,2
D3: Gestión para Resultados	53,2	98,1
D4: Evaluación de Resultados	59,8	98,8
D5: Información y Comunicación	50,2	98,6
D6: Gestión del conocimiento	63,2	99,1
D7: Control Interno	51,3	98,3

Nota: Para el filtro o consulta de una sola entidad, el máximo corresponden al puntaje máximo obtenido por entidades del grupo par al que pertenece la entidad objeto de consulta. Para los demás filtros, estos valores corresponden al puntaje máximo del total de entidades del orden territorial.

III. Índices de las políticas de gestión y desempeño

Consulte aquí recomendaciones de mejora por entidad

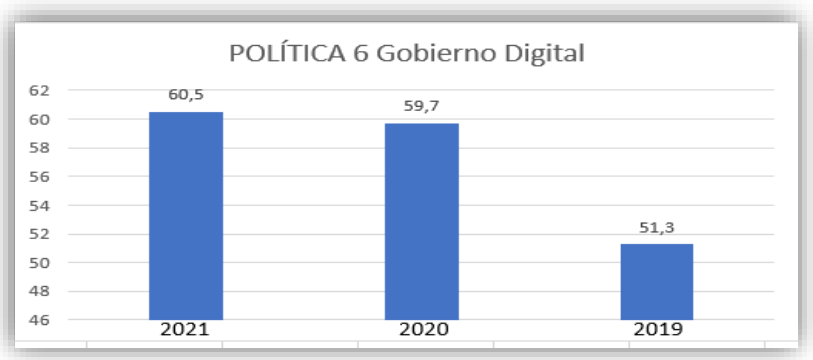


Nota: Los colores en este gráfico representan un ranking de las políticas según los puntajes obtenidos. No necesariamente determinan un alto o bajo desempeño.

POL01: Gestión Estratégica del Talento Humano
POL02: Integridad
POL03: Planeación Institucional
POL05: Fortalecimiento Organizacional y Simplificación de Procesos
POL06: Gobierno Digital
POL07: Seguridad Digital
POL09: Transparencia, Acceso a la Informa lucha contra la Corrupción
POL10: Servicio al ciudadano
POL11: Racionalización de Trámites
POL12: Participación Ciudadana en la Ges Pública
POL13: Seguimiento y Evaluación del Desempeño Institucional
POL14: Gestión Documental
POL15: Gestión del conocimiento
POL16: Control Interno

IV. Índices detallados por política

Índices detallados por política de gestión y desempeño institucional	Puntaje consultado	Valor máximo de referencia
GOBIERNO DIGITAL: Empoderamiento de los ciudadanos mediante un Estado abierto	69,3	96,8
GOBIERNO DIGITAL: Fortalecimiento de la Arquitectura Empresarial y de la Gestión de TI	43,2	98,3
GOBIERNO DIGITAL: Fortalecimiento de la Seguridad y Privacidad de la Información	25,5	99,3
GOBIERNO DIGITAL: Procesos seguros y eficientes	55,9	84,4
GOBIERNO DIGITAL: Servicios Digitales de Confianza y Calidad	95,4	99,8
GOBIERNO DIGITAL: Toma de decisiones basadas en datos	49,4	98,6
GOBIERNO DIGITAL: Uso y apropiación de los Servicios Ciudadanos Digitales	42,1	94,8



De acuerdo a las gráficas anteriores, podemos observar que la política de gobierno digital en el año 2020 obtuvo una calificación de 59.7, frente al 2021 con una calificación de 60.5, lo que evidencia la constancia y eficacia en la ejecución de las estrategias implementadas para la mejora de las políticas en mención.

Sin embargo, al verificar la gráfica IV. Índices detallados por política, se puede observar que los habilitadores “Fortalecimiento de la seguridad y privacidad de la información” obtuvo la calificación de 25.5 puntos, observando la calificación más baja de la política, lo que evidencia una necesidad imperiosa de diseñar estrategias efectivas para la mejora de la política y garantizar su adecuada implementación.

2.6 Otros aspectos - TERMINOS Y DEFINICIONES

- ✓ **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- ✓ **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- ✓ **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- ✓ **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- ✓ **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000). Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).

- ✓ **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).
- ✓ **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).
- ✓ **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).
- ✓ **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 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.
- ✓ **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- ✓ **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación.
- ✓ **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- ✓ **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. (ISO/IEC 27000).

2.7 Recursos y responsables

Recursos:

Humano: la Dirección, Líderes de los Procesos.

Físico: Servidores, Firewall, PC y equipos de comunicación

Financiero: Plan de Adquisiciones

Responsables

Dirección

Líderes de los Proceso

Comité del sistema de Gestión de la Información

2.8 Metodología de Implementación

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en el Inderhuila, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Manual de implementación versión 3.02 del Ministerio de Tecnologías de la Información y las Comunicaciones.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

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

Fuente: Manual Modelo de seguridad y Privacidad de la Información – MinTIc

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar para la implementación de acuerdo a lo establecido por el Inderhuila:

- Implementar la Política de Seguridad de la información.
- Implementar la Política de Administración de datos.
- Implementar la Políticas de Comunicaciones.
- Aspectos organizativos de la seguridad de la información
- Seguridad de la Información enfocada a los recursos humanos.
- Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

- Revisión de los Controles de acceso Seguridad Física y del entorno Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Anexo: Formulación del Plan de Acción de la Estrategia (formato código DIH-CDEP-P01-F01)

SUBCOMPONENTE	DISEÑE ALTERNATIVAS DE MEJORA	META/PRODUCTO	NOMBRE DEL INDICADOR	FÓRMULA DEL CÁLCULO Y PERIODICIDAD	2do Trimestre 30- MAY	3er Trimestre 30-AGO	4to Trimestre 30-NOV	PRODUCTO / ENTREGABLE	PLAZO DE REALIZACIÓN DE LAS ACTIVIDADES (INICIO-FIN)	LIDER RESPONSABLE DE LA TAREA
FORTALECIMIENTO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Realizar un diagnóstico de seguridad y privacidad de la información para la vigencia 2023.	Un diagnóstico (MSPI)	N/A	N/A				Diagnóstico construido herramienta MPSI	01-02-2023 al 30-03-2023	Líder TIC
IMPLEMENTAR LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Elaborar la política de las buenas prácticas.	Realizar evaluación semestral al 70% de funcionarios y contratistas administrativos.	Porcentaje de funcionarios y contratistas que respondieron la evaluación	No. Evaluaciones aplicadas/Total de funcionarios y contratistas				Resultado de las evaluaciones	01-02-2023 al 30-11-2023	Líder TIC
	Realizar Inventario de Activos de Información con los líderes de cada Proceso.	Realizar el inventario al 50% de los procesos.	Cantidad de procesos con activos de información identificados	No. De procesos con activos de información identificados/ Total procesos de la entidad				Matriz con la información de activos de información.	01-02-2023 al 30-11-2023	Líder TIC
	Una vez identificado los activos de información realizar el plan de tratamiento de riesgos	Realizar el tratamiento de riesgos al 50% de los activos de información identificados.	Plan de tratamientos de riesgos	No. activos de información con tratamiento de riesgos/ Total de activos de información				Matriz del plan de tratamiento de riesgos de activos de información	01-02-2023 al 30-11-2023	Líder TIC
	Socializar el plan de tratamiento de riesgos	Socializar al 100% del personal administrativo del Inderhuila el plan de tratamiento de riesgos	Socialización plan de tratamiento de riesgos	No. Cantidad de personal administrativo a los que se le socializó el plan de tratamiento de riesgos / No. Total personal administrativo				Acta de socialización del plan de tratamiento de riesgos	01-02-2023 al 30-11-2023	Líder TIC

1. CONCLUSIONES

Se identifica la necesidad apremiante de establecer y documentar lineamientos internos de seguridad y privacidad de la información, que faciliten la implementación de medidas y controles para la gestión de la información y los activos de TI de la entidad, a fin de optimizar los procesos.

Respecto al talento humano, el INDERHUILA capacitará al personal en buenas prácticas de seguridad de la información, para que a su vez permita crear, difundir y establecer una cultura organizacional en esta materia entre los funcionarios y áreas de la entidad.

MAURO SAUL SANCHEZ ZAMBRANO
Director Inderhuila

Redacto
Cruzval Alberto Rodriguez M
Ingeniero de Sistemas