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

ENERO DE 2023

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Proceso: COMUNICACIONES ESTRATÉGICAS Y TIC

INDERHUILA

TABLA DE CONTENIDO

INTRODUCCIÓN

La Política de la seguridad de la información del **INDERHUILA,** asegura que la organización establezca la protección de los activos de información (funcionarios, contratistas, partes interesadas, la información, los procesos, las tecnologías de información incluido el hardware y el software) dando cumplimiento a los requisitos establecidos por las partes interesadas en la gestión de la Información.

Además, tiene como propósito salvaguardar la información generada dentro de la entidad garantizando así la seguridad de los datos y dando cumplimiento a la normatividad legal vigente, para poder realizar un Plan de Seguridad y Privacidad de la información con el fin de que no se presenten robos, perdidas de información, accesos no autorizados y duplicación de información que puedan ocasionar daños a los usuarios tanto internos como externos.

1. CONTEXTO ESTRATÉGICO

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 ESTRATEGIA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1 MARCO LEGAL

MARCO NORMATIVO	DESCRIPCION
Ley 527/99	"Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos"
Ley 1266/08	"Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".
Ley 1581/12	"Por la cual se dictan disposiciones generales para la protección de datos personales".
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 1499 del 11 de septiembre de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 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.

2.2 ALCANCE

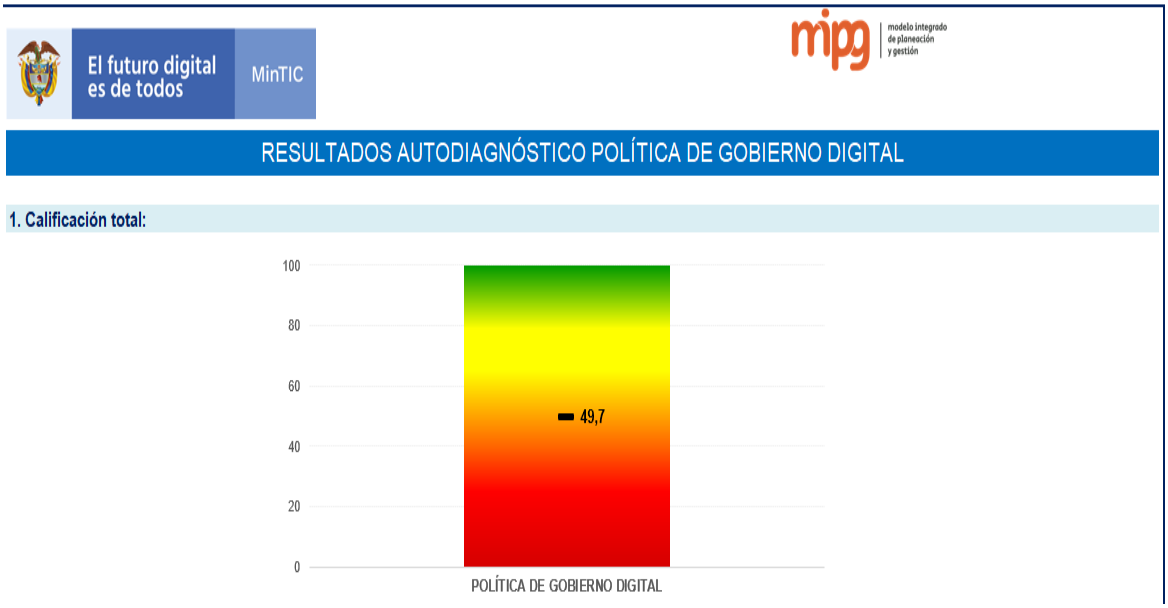
El plan de Seguridad y Privacidad de la información comprende todos los activos de información del INDERHUILA, y la totalidad de los procesos y actividades del sistema de gestión: Modelo Integrado de Planeación y Gestión – MIPG, que permitan adoptar políticas y procedimientos que se establezcan sobre dichos activos, enmarcados en un ciclo PHVA, con el fin de mejorar la eficacia y eficiencia de los servicios ofertados a la ciudadanía.

2.3 OBJETIVOS

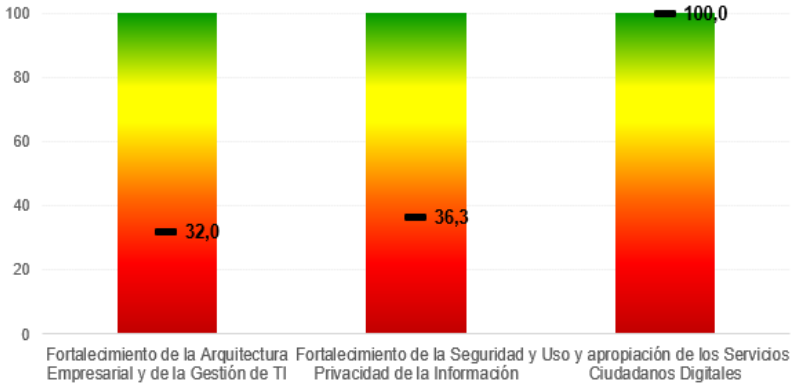
- Implementar los activos de Información del Inderhuila
- Identificar los riesgos de los activos de Información
- Realizar el tratamiento de los datos a los riesgos identificados

2.4 DIAGNÓSTICO DE LA POLÍTICA

Una vez realizado 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 puntos; en el cual se evaluaron los tres 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:



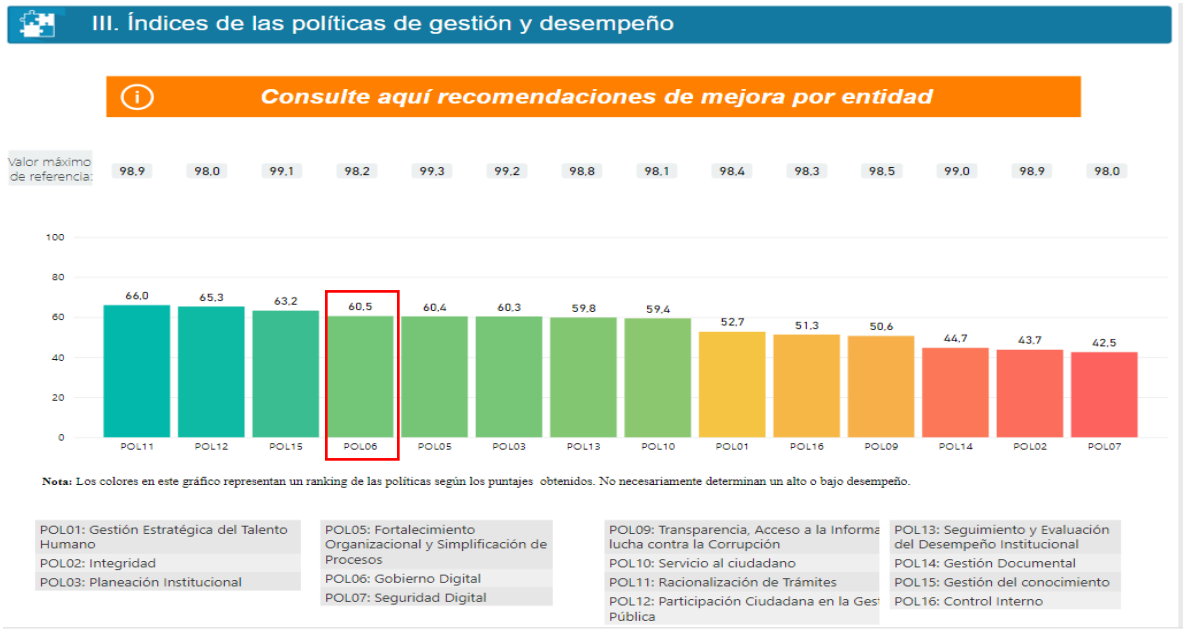
Por lo anterior, resulta imperiosa implementar estrategias para desarrollar la Política de Gobierno Digital para dar lugar al fortalecimiento de la seguridad y privacidad de la información, fortalecimiento de la arquitectura empresarial y de la gestión de TI y apropiación de los servicios ciudadanos digitales, con el objetivo de aumentar la puntuación en general, especialmente en los dos habilitadores que obtuvieron una puntuación critica de 32 y 36.3, 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 enfocando sus esfuerzos para generar valor público a nuestros grupos de valor.

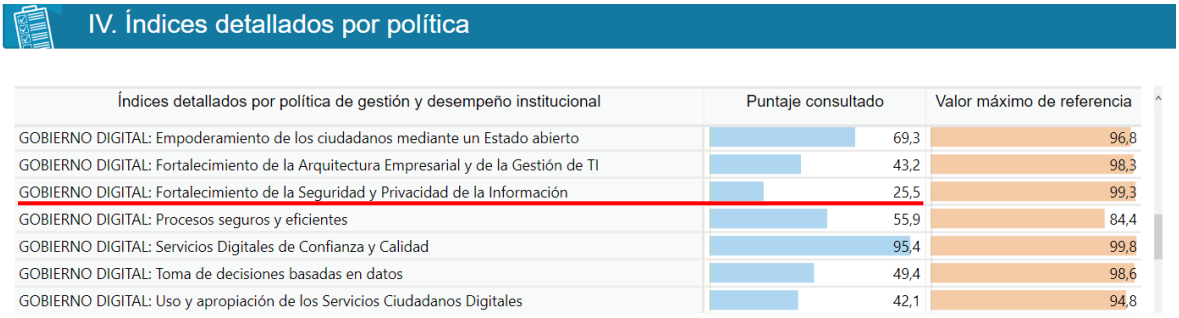
2.5 RESULTADOS MEDICIÓN FORMULARIO ÚNICO REPORTE DE AVANCES DE LA GESTIÓN – FURAG

II. Índices de las dimensiones de gestión y desempeño

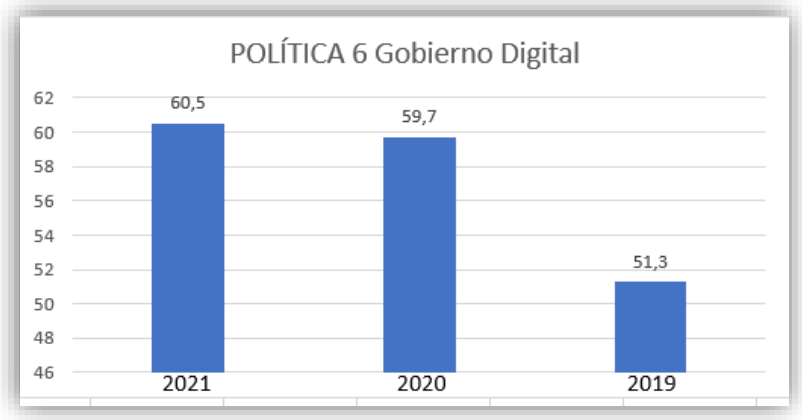
Dimensión	Puntaje consultado	Valor máximo de referencia
D1: Talento Humano	49,2	98,4
D2: Direccionamiento y Planeación	60,3	99,2
D3: Gestión para Resultados	53,2	98,1
D4: Evaluación de Resultados	59,8	98,8
D5: Información y Comunicación	50,2	98,6
D6: Gestión del conocimiento	63,2	99,1
D7: Control Interno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





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, observando una variación positiva de 0.8, lo que evidencia la constancia en la ejecución de las estrategias implementadas para la política gobierno digital.

Sin embargo, al verificar la gráfica IV. Índices detallados por política, se puede observar que el habilitador “Fortalecimiento de la seguridad y privacidad de la información” obtuvo la calificación más baja con 25.5 puntos, 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: PRINCIPIOS

a) Para el INDERHUILA es importante generar políticas de la Seguridad de la Información cuyo fin es brindar orientación y soporte por parte de la dirección para dar cumplimiento con los requisitos de la entidad, las leyes y demás reglamentarios pertinentes.

c) La Integridad de la información del INDERHUILA debe preservar siempre su autenticidad manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

d) La Disponibilidad de la Información del INDERHUILA debe estar disponible cuando sea requerida por cualquier parte interesada.

e) La confidencialidad de la información del INDERHUILA es garantizar que la información personal será protegida y accedida solo por aquellos que estén involucrados en dicha información y no será divulgada sin consentimiento ninguno.

f) La privacidad del INDERHUILA debe estar preservada con el fin de que sea utilizadas para los propósitos que fue generada.

2.7 TERMINOS Y DEFINICIIONES

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 entidad. (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.

Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).

Partes interesadas: 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).

Vulnerabilidad: Vulnerabilidad es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales

2.8 RESPONBLES

El **INDERHUILA** tiene como responsables de la implementación, seguimiento y mantenimiento de la Política del Plan de Seguridad y Privacidad de la información lo siguiente:

El representante de la dirección del INDERHUILA, quien velará por el cumplimiento de la Política de Seguridad y privacidad de la Información.

El profesional Universitario encargado de la gestión de TICS, será el encargado de desarrollar la implementación de la Política de seguridad y privacidad de la información y quien velará la formulación e implementación de la Política de seguridad y privacidad de la información.

Todos los funcionarios y/o contratistas y demás partes interesadas del INDERHUILA son responsables del cumplimiento obligatorio de la Política de seguridad y Privacidad de la Información y en caso de no cumplir se reserva el derecho de tomar las medidas correspondientes según el caso.

Para comunicar esta política se hará mediante socialización con todos los funcionarios, contratista y partes interesadas del INDERHUILA, el cual dará a conocer la existencia, contenido y obligatoriedad de dicho documento. La custodia y ubicación física del documento estará a cargo del Sistema de Gestión: Modelo Integrado de Planeación y Gestión y el líder de TIC.

2.9 POLÍTICA

El INDERHUILA divulgará los objetivos y alcances de la seguridad de la información dentro de la entidad, que son efectivos por medio de controles de seguridad, con el fin de mantener, gestionar y mitigar el riesgo como se estable en el Plan de Tratamiento de Riesgos, según norma ISO 27001, garantizando así la continuidad de los servicios y disminuyendo la probabilidad de amenazas que puedan afectar los procesos internos para el cumplimiento de la prestación del servicio.

Identificación, clasificación y valoración de activos de información:

Debe ser compromiso de la administración realizar el inventario de activos del INDERHUILA donde se incorpore la clasificación, valoración, ubicación y acceso de la información y demás características identificas por la dirección.

Seguridad de la información en el Talento Humano:

Todas y todos los servidores públicos del INDERHUILA, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. Por ende, se debe contar con un directorio completo y actualizado de los perfiles creados.

La responsabilidad de custodia de cualquier documento o archivo generado dentro de la entidad, usado o producido por algún funcionario y/o contratista que se retira, o cambia de cargo, recae en el profesional Universitario encargado de la gestión de TICS y supervisor del contrato; aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

Usuarios invitados y servicios de acceso público

El acceso de usuarios no registrados solo debe estar autorizado por la dirección, de manera de información institucional, igualmente el servicio de internet al que puedan acceder debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

Seguridad Física y del entorno

Seguridad en los equipos: Los servidores o equipos de cómputo que contengan informaciones institucionales deben estar en un ambiente seguro y protegido por lo menos con:

- Controles de acceso y seguridad física.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Además, toda información institucional en formato digital debe ser mantenida en los servidores propios o contratados y/o unidades extraíbles aprobados por el profesional Universitario encargado de la gestión de TICS.

También se debe asegurar que la infraestructura esté cubierta, con mantenimiento y soporte adecuados tanto para el hardware como para el software y las estaciones de trabajo deben ser operadas por funcionarios de la institución el cual deben estar capacitados acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Se deben incluir los medios que alojan copias de seguridad el cual deben ser conservados de forma correcta de acuerdo a las políticas y estándares establecidos.

Administración de las comunicaciones y operaciones

Reporte y revisión de incidentes de seguridad: El personal vinculado al INDERHUILA, debe realizar el reporte de una manera eficiente y con responsabilidad de las presuntas violaciones de seguridad detectadas y se deben reportar a través de su supervisor al profesional Universitario encargado de la gestión de TICS o cuando la ocasión lo amerite si es un caso especial y podrá realizarse directamente por la persona que encuentre el incidente o novedad.

Se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad el cual se mantendrá procedimientos escritos para la operación de dichas actividades sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información.

Protección contra software malicioso y hacking.

Se debe proteger todos los sistemas de información que involucre los controles humanos, físicos técnicos y administrativos para no incurrir en daños, se elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que pueda afectar la prestación del servicio.

Como control básico, se debe instalar una IP fija en el Router, y todas las estaciones de trabajo del INDERHUILA, deben estar protegidas por antivirus licenciados, y el router debe tener instalado un VPN licenciado.

Copias de Seguridad

Toda información que sea de interés para un proceso siempre debe estar respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados y probados por el Sistema Integrado de Gestión.

El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro que se deben efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir la responsabilidad de realizar las copias y mantenerlas actualizadas, recae directamente sobre cada dueño de los activos de la información de la Entidad.

Intercambio de Información con Entidades Externas

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la dirección, y ser redireccionados a los responsables del manejo y custodia dicha información. Tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha aclarando que toda información institucional debe ser manejada de acuerdo a la normatividad legal vigente.

Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados en al INDERHUILA, deben ser aprobadas por la dirección, de acuerdo a los procedimientos establecidos para tal fin.

El funcionario encargado en la Gestión de las TIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad para su respectiva investigación además debe tener un inventario del software autorizado para su uso institucional.

Control de Claves y Nombres de Usuario

Las claves de administrador de los diferentes sistemas deben ser conservadas por el profesional Universitario encargado de la gestión de TICS y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Adicionalmente se debe elaborar, mantener y actualizar el procedimiento para la correcta definición, uso y complejidad de las claves de usuario.

Una vez se termine la relación contractual o laboral del personal con el INDERHUILA, se debe expedir un certificado de suspensión y/o cancelación de las cuentas creadas al respectivo usuario, en todos y cada uno de los sistemas de información en los cuales estuviera activo (correo electrónico, sistemas de información automatizados, entre otros); se determinara cual será el tiempo prudencial por la posible renovación de la relación contractual o laboral, o una vez transcurrido el tiempo se dará de baja las cuentas si no hay renovación ninguna.

Uso adecuado de Internet

El INDERHUILA es consciente de la importancia del servicio de Internet como una herramienta fundamental para el desempeño de labores que proporcionará los recursos necesarios para asegurar su disponibilidad a los servidores públicos y demás partes de interés que así lo requieran.

a. El proceso de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
b. El proceso de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
c. El proceso de TIC debe monitorear continuamente el canal o canales del servicio de Internet.

3. CONCLUSIONES

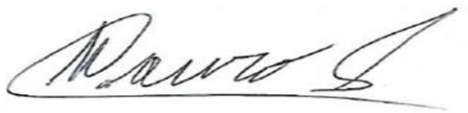
La implementación de un Plan Estratégico de Tecnología de Información PETI por parte de la Inderhuila, ha conllevado a la variación de los componentes operativos y de Tecnología de la Información (TI), como son en la implementación del sistema de gestión de la seguridad de la información (SGSI). Este sistema fortalecerá la institución en su infraestructura física y lógica, y obtendrá los riesgos de la información de la entidad. La información es un valor que se transforma en un factor crítico de éxito hoy en día, pues gracias a ella se pueden tomar decisiones que van a repercutir en las

diversas unidades y departamentos para apoyar la estrategia de la organización. El PETI se encarga de administrar eficientemente el manejo de la información garantizando la concordancia de la estrategia de la institución y la estrategia de TI.

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

Plan de acción inderhuila 2022		
ITEM	**DETALLE**	**FECHA**
1	Capacitar y sensibilizar al personal sobre la importancia que tiene realizar el procedimiento del Backup según el procedimiento	10/01/ al 30/06/2023
2	Fortalecer físicamente el cableado de la red de datos, adecuar el sitio donde está el Modem de claro para proteger los equipos de daños físicos, mal intencionados y lógicos.	10/01/ al 30/06/2023
3	Mejorar el Sistema de cableado de red del	10/01/ al 30/12/2023
4	Cambiar el Operador de Internet para lograr una mayor capacidad de cobertura para cada una de las áreas del Inderhuila	10/01/ al 30/06/2023
5	Todos los computadores servidores, portátiles y computadores de mesa deberán tener una contraseña instalada por el usuario pero debe ser de conocimiento de esta a la dependencia de las Tic, cada novedad debe ser informada.	10/01/ al 30/06/2023



MAURO SAUL SANCHEZ ZAMBRANO
Director Inderhuila

Redacto
Cruzval Alberto Rodriguez M
Ingeniero de Sistemas