INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI PROCESO GESTIÓN ADMINISTRATIVA	CODIGO	PA-PL-242-004
		VERSIÓN	2
		APROBADO	10/MAR/2021

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN - PETI

INDERVALLE

2020-2023

INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN **PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI** **PROCESO GESTIÓN ADMINISTRATIVA**	CODIGO	PA-PL-242-004
		VERSIÓN	2
		APROBADO	10/MAR/2021

Contenido

1. INTRODUCCIÓN

La Planeación Estratégica De Tecnologías De La Información - PETI, tienen como objetivo asegurar que las metas y objetivos de las Tecnología de la Información, TI estén vinculados y alineados con las metas y objetivos de la Entidad.

Es un proceso dinámico e interactivo para estructurar estratégica, táctica y operacionalmente la infraestructura de las Tecnología de la Información, TI y los sistemas de información que soporten la gestión de INDERVALLE.

La planeación estratégica de las Tecnología de la Información, TI, puede ser definida como "la planeación para el manejo efectivo de la información en todas sus formas – sistemas de información y tecnología; sistemas manuales y computarizados; tecnología de cómputo y telecomunicaciones – la cual incluyen aspectos organizacionales de administración de TIC a través de todo el negocio" [Ward & Griffiths 1996].

Vigencia

El presente Plan Estratégico de Tecnologías de La Información, PETI, cuenta con una vigencia de 4 años para el periodo 2020- 2023 enmarcada en el periodo de gobierno y alineado con el Plan Estratégico Institucional, permitiendo revisiones periódicas siempre que sea necesario para alinear o ajustar sus metas de acuerdo con las directrices del Gobierno.

2. OBJETIVO ESTRATÉGICO

Promover el desarrollo sostenible de INDERVALLE a partir de la modernización de la entidad, apoyados en el uso estratégico de las Tecnologías de la Información y la Comunicación, TIC, para contribuir en la construcción de un gobierno más eficiente, transparente, participativo, cercano y que genere progreso al departamento.

2.1. Objetivos específicos

- Implementar un gobierno corporativo de las tecnologías de la información y las comunicaciones en INDERVALLE, a través del cual se dirige y controla el uso actual y futuro de dichas tecnologías.
- Fortalecer la gestión e interoperabilidad de INDERVALLE en aceptación de sus dependencias y los intereses de la ciudad a través de las tecnologías de la información y la comunicación.
- Incrementar la calidad y cantidad de los servicios en línea ofrecidos a los ciudadanos.
- Promover la veeduría ciudadana a través de herramientas tecnológicas.
- Implementar un sistema de Gestión de Seguridad de la Información que le permita a INDERVALLE salvaguardar la información.

3. ALCANCE DEL DOCUMENTO

El Plan Estratégico de Tecnologías de la Información, PETI, se formuló considerando la parte institucional en la cual se gestionan los procesos de la entidad con la tecnología para generar valor y cumplir de manera efectiva las metas del Plan De Desarrollo Departamental "El Valle Está En Vos" y la misión con la que cuenta INDERVALLE, por otro lado en la participación y acercamiento con la ciudadanía ampliando y mejorando la calidad y cantidad de servicios en línea el cual incrementa la calidad de vida de los ciudadanos.

El Plan Estratégico de Tecnologías de la información está comprendido por cuatro, (4) fases:

En la primera fase, se lleva a cabo el análisis de la situación actual, a través del entendimiento general de la estrategia organizacional, de la construcción de los procesos, del grado de madurez actual en la gestión de las tecnologías de la Información, TI y de la aceptación de la tecnología como herramienta de avance para la entidad.

La segunda fase comprende el análisis del modelo operativo y organizacional de la entidad, las necesidades de información y la alineación de tecnologías de la información, TI, con los procesos, de tal forma que se tenga plena conciencia de los cambios o ajustes que se realizan al respecto, preparando el desarrollo de la estrategia de tecnologías de la información, TI.

En la tercera fase, a partir del entendimiento logrado en las dos fases anteriores, se desarrolla la estrategia de TI, la cual plantea el modelo de gestión de TI, arquitectura de servicios tecnológicos, Gobierno de TI y modelos de uso y apropiación, teniendo en cuenta no sólo los aspectos intrínsecos de cada componente, sino las actividades estratégicas transversales a la gestión de TI.

Finalmente, en la cuarta fase se establece el modelo de planeación con la definición de los lineamientos y actividades estratégicas para desarrollar el plan de implementación de la estrategia y se estructura del plan maestro. Teniendo en cuenta los lineamientos, se desarrollan los planes de acción en el corto, mediano y largo plazo, con actualizaciones anuales que tomarán en cuenta los avances en los proyectos que lo componen y el contexto en el que se desarrollan.

4. MARCO NORMATIVO

- Decreto Nacional 2573 de 2014 Lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Concordancias; Decreto 1078 del 2015, se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
- Decreto 1151 de 2008 se estableció como objetivo de la Estrategia Gobierno en Línea "Contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación".
- Decreto 1008 de 2018, Política de Gobierno Digital, (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG).
- Ley 489 de 1998, artículo 39, Política de Gobierno Digital en la Administración Pública y los particulares que cumplen funciones administrativas.

5. RUPTURAS ESTRATÉGICAS

Las rupturas estratégicas nos permiten identificar los **PARADIGMAS A ROMPER** de la Institución pública para llevar a cabo la transformación de la gestión de TI, a continuación, se listan las siguientes rupturas estratégicas identificadas:

- La tecnología debe ser considerada un factor de valor estratégico para la institución pública.
- Las áreas misionales deben apuntar a resolver problemas mediante sistemas de información.
- La seguridad de la información no es necesaria porque la entidad, no es un banco.
- Necesidad de liderazgo al interior de la institución pública para la gestión de Sistemas de Información, se debe de Contar con una oficina de TI, que haga parte del Comité Directivo, que gerencia las actividades, los recursos y que se enfoque hacia un servicio de la mejor calidad posible, para los clientes internos y externos.
- Los proyectos de Tecnología de la Información, TI son costosos y no siempre es claro su retorno de inversión.
- Alinear las soluciones con los procesos, aprovechando las oportunidades de la tecnología, según el costo/beneficio
- Los sistemas de información no se integran y no facilitan las acciones coordinadas.
- Hay una amplia brecha entre los directivos y el personal de Tecnología de la Información, TI.
- Resolver el dilema entre "desarrollar en casa" vs. "Comprar software comercial".

6. ESTRUCTURA ORGANIZACIONAL

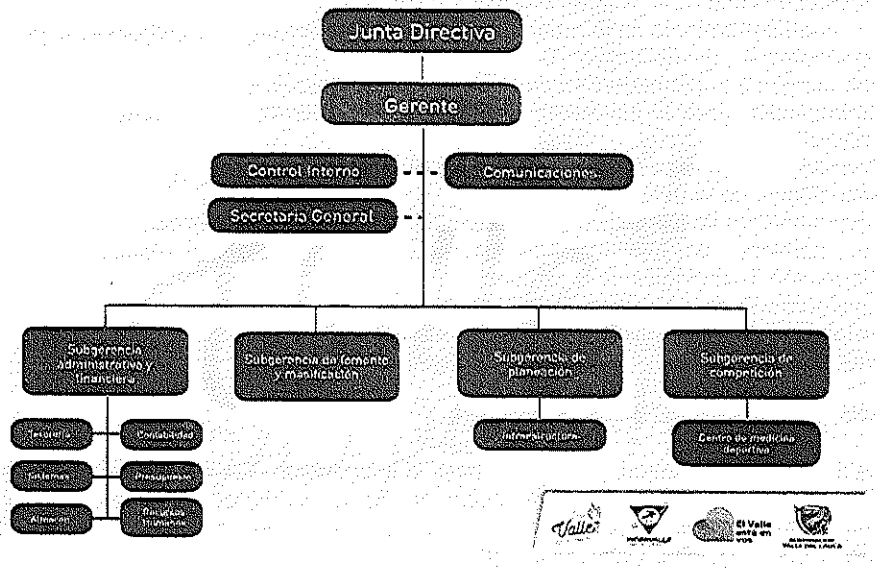


Imagen 1. Organigrama institucional. Fuente: www.INDERVALLE.gov.co

Se observa el área TIC, de la entidad como área de **Sistemas**, componente de apoyo a la gestión de INDERVALLE desde la Subgerencia Administrativa y Financiera, para la gestión corporativa en los procesos de Tecnologías de la Información y Comunicaciones.

El área debe establecer un organigrama desde su área para definir responsabilidades de cargos y asignación de actividades. De esta forma inicia el proceso de cambio y apuntando así a establecer un modelo de arquitectura empresarial.

Las actividades del área se centran en la información suministrada por entidad, esto debe implementar el catálogo de servicios tecnológicos de la entidad y los procesos y procedimientos actualizados.

a. Elaboración y socialización de los diferentes Planes, procesos y procedimientos del área.
b. Mantenimiento preventivo y correctivo de la plataforma tecnológica, el cual se actualiza como Gestión de las TICS.
c. Actualización de la red LAN, corresponde a la actualización del cableado estructurado y el cumplimiento de los estándares internacionales.
d. Administración aplicativo SIGDOCs en sus módulos de ventanilla única y PQRSD
e. Administración del sitio web de la Entidad, donde se publican todas las actividades desarrolladas por la misma.
f. Administración de los correos institucionales utilizados por los funcionarios de la Entidad:
   - Capacidad de almacenamiento.
   - Permiso o no de inicio de sesión, permiso de envío de correos, entre otros.
g. Administración y/o configuración de la red interna de la Entidad, es decir, todos los dispositivos que permiten la conexión a Internet, tales como Access Point, Switch..)
h. Configuración de las diferentes impresoras multifuncionales de la entidad, para que esta se encuentre en red con los diferentes equipos de cómputo pertenecientes a la misma.
i. Servicio de Help Desk soporte técnico:
   - Acompañamiento en la reparación de los diferentes equipos tecnológicos de La Entidad.
j. Administración del aplicativo V6 – Financiero y Contable.
k. Elaboración e Implementación de Formatos para el desarrollo de las funciones del área.
l. Coordinación para la instalación del servicio de Internet en las sedes pertenecientes a La Entidad.
m. Conciliación con área del Almacén de los equipos de cómputo pertenecientes a la Plataforma Tecnológica de la Entidad
n. Levantamiento de las necesidades tecnológicas de las diferentes dependencias de la entidad.
o. Levantamiento de Inventario de los recursos tecnológicos o medios tecnológicos de la Plataforma Tecnológica de la Entidad.
p. Configuración del Equipo DVR de La Entidad
q. Instalación, Configuración y puesta en marcha de los diferentes equipos tecnológicos de la entidad.

7. ANÁLISIS DE LA SITUACIÓN ACTUAL

El análisis de la situación actual, tiene como base la información histórica de la entidad, además de la recolección de la información, la observación de las necesidades establecidas y el diagnostico presentando por la consultoría realizado por el convenio interadministrativo 3092-2020 en el cual su informe presenta la siguiente situación actual:

INFORME TÉCNICO DE EJECUCIÓN:

En la actualidad INDERVALLE cuenta con una arquitectura existente para la prestación de servicios internos que a las diferentes áreas que componen la institución. Toda arquitectura existente a medida que pasa el tiempo requiere mantenimiento y actualización hasta cumplir con el ciclo de vida provisto desde el punto inicio y puesta en marcha.

Desde el montaje de un sistema se prevé cual será la vida útil y pese a los esfuerzos por sobre ponerse en el tiempo la renovación tecnológica los sistemas evolucionan cada día y con ello los servicios que corren sobre estas nuevas plataformas exigen que la infraestructura sobre la que se prestan diferentes servicios se actualice para soportar la nueva carga impuesta por los consumidores de contenidos.

Debido a ello las instituciones deben mejorar la plataforma tecnológica con el fin de proveer más servicios con mejor eficiencia y con calidad de servicio. Para ello junto con el área de TI en cabeza de la Ing. Stella Jiménez se determinará mediante estudio técnico la ruta sobre la cual la institución deberá prever el crecimiento tecnológico y de servicios puestos a los diferentes actores internos y externos que interactúan con la institución.
Situación Actual: La institución cuenta con una plataforma de redes de varias generaciones lo cual a medida que ha pasado el tiempo se vienen actualizando no de la manera organizada que el ejercicio requiere basado en un plan de desarrollo sino de la necesidad expresada en el momento donde se formulan las necesidades de expansión de red para brindar conectividad con el fin de proveer servicios. Debido a la mezcla que se presenta en la actualidad existen protocolos y configuraciones que en nuestros días no serán convenientes para dar una dinámica de crecimiento escalonado y cambiante dentro de un entorno educativo donde las mejoras, los cambios, la innovación debe ser la cúspide para lograr la interacción entre los componentes de investigación y desarrollo que provienen de grupos interdisciplinarios y para ello se requiere reestructurar la plataforma que soporta toda la capa de servicios prestados a una de última tecnología.

Dentro del esquema actual se pueden presentar vulnerabilidades a nivel de seguridad lógica lo que deja en descubierto todos los sistemas críticos dentro de la institución. Esquemas con falencias basados en calidad de servicio, redes no basadas en esquemas virtuales dificultan el crecimiento y administración.

PROCESOS:

- infraestructura física
- infraestructura lógica
- Sistemas de procesamiento, información y almacenamiento
- Sistemas de protección eléctrica y enfriamiento.

1. **INFRAESTRUCTURA FÍSICA:** Como primera fase del proyecto se identificaron los sistemas de redes existentes encontrando lo siguiente:
    a. Cables de cobre cat5
    b. Cables de cobre cat5E
    c. Cables de cobre cat6

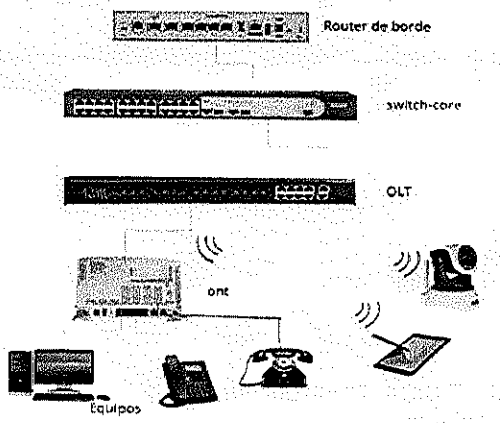
Como se pudo observar en las visitas realizadas a las instalaciones tenemos varios tipos de generaciones de cables de cobre lo cual afecta el rendimiento de red para todo el ecosistema.

La obsolescencia del cable atribuye a formar cuellos de botella en el desempeño de las redes, esto debido a la manufactura y componentes además de otros factores que implican las redes de cobre como son:

- Desfase. Variación de la velocidad de propagación de la señal en función de la frecuencia.
- Interferencia electromagnética (ruido): – Externa (motores, emisiones de radio y TV, etc.). De señales paralelas: diafonía o crosstalk (efecto de cruce de líneas). La diafonía puede ser:
  - Del extremo cercano. Ratio NEXT (Near End Crosstalk): Señal Referencia - señal inducida en el lado del emisor
  - Del extremo lejano. Ratio FEXT (Far End Crosstalk): Señal Referencia - señal inducida en el lado receptor – La diafonía aumenta con la frecuencia
- Distancia en cables de cobre para redes LAN no se pueden superar los 100 metros incluyendo los patchcord de conexión a los adaptadores de red de los pc y switches.

Para la modernización tecnológica a nivel de redes tenemos:
Tecnología conocida como FTTH (Fiber to the Home) o FTTD (Fiber to the Desk) fue creada para atender un segmento del mercado como son: centros de concentración urbana y sector corporativo, principalmente grandes superficies como edificios gubernamentales, universidades, plantas industriales, urbanizaciones en conjunto cerrado o edificios de apartamentos, aeropuertos, hoteles y bases militares. Es una solución innovadora de infraestructura de redes aplicada a Redes de Áreas Locales (LAN), adaptados a esta tecnología para la distribución de servicios avanzados tales como: VOIP (Voz sobre IP), HDTV (Televisión digital de alta definición), VOD (Vídeo bajo demanda), Internet de banda ancha sin restricciones de distancias y velocidad, Juegos en red y Video llamada, redes P2P.

Imagen ilustrativa de red basada en FO.



Características de red en fibra óptica:

- La distancia física máxima entre la OLT y las ONT´s puede ser de 20 km, o sea, 200 veces más que la distancia máxima prevista en norma para el cableado tradicional, los proyectos con Solución GPON LAN eliminan significativamente la cantidad de cuartos de equipos y centros de cableado cuando se compara con la solución convencional.
- La cantidad de cableado en fibra es mucho menor por el hecho que cada fibra puede transportar información y servicios de varios usuarios en un único hilo, característica principal de un sistema punto- multipunto.

- Menor Consumo de Energía en función de la no utilización de equipos activos intermedios, al no existir equipos activos, no se requiere de equipos para refrigeración ni suministro de energía en los cuartos alternos. En los cuartos alternos solo se instalarán equipos pasivos, es decir no requieren fuente de energía y por lo tanto no generan calor térmico, entonces tampoco requieren refrigeración.

2. **INFRAESTRUCTURA LOGICA:** Como segunda fase se identificaron los elementos activos de red existentes dentro de las instalaciones de los que encontramos los siguientes:

Los switches encontrados dentro de las instalaciones son de tipo redes domésticas o de pequeñas empresas sin administración ni manejo de vlan para segmentación de tráfico en la red.

Dentro del edificio encontramos estos tres como principales para distribución:

- TP-Link TLSG-1024D Giga
- TP-Link TLSF-1024D Fast Ethernet
- TrendNet TEDS26g

No existen equipos de protección como firewall o UTM.

No existe red inalámbrica corporativa.

Para garantizar una correcta operación de los sistemas se deben perfeccionar los elementos activos que conforman la red, esto garantizara niveles de estabilidad, protección y conectividad de alto nivel para todas las dependencias de la institución.

Como plan de mejoramiento se propone:

- El uso de switches de nivel corporativo los cuales cuentan con administración, segmentación y QoS.
  ¿Por qué una segmentación de redes?

  La segmentación de red es una estrategia que permite dividir las redes que forman parte de un sistema en "zonas de seguridad" o segmentos separados por cortafuegos. Cuando se configura correctamente; los segmentos separan las aplicaciones y evitan el acceso a los datos confidenciales.

  Los sistemas corporativos tienden a enfrentarse constantemente a grandes retos para mantener la seguridad de sus redes. Esto es principalmente gracias a que en la red interactúan una enorme cantidad de datos; protegidos muchas veces por estrategias de seguridad poco sólidas.

  Considerando que entre estos datos se puede encontrar información sensible de clientes o de la misma empresa; no resulta sorprendente que los cibercriminales usen las redes como objetivo principal para el robo de datos.

- El uso de sistema de protección perimetral (firewall y/o UTM) nos permiten prevenir riesgos de infiltración de la red a nivel externo e interno.

¿Porque usar un firewall?
La información es tan importante para lograr los objetivos en las organizaciones, que es considerada el activo más importante. Por eso, es objeto de diversas amenazas, como el robo, la falsificación, el fraude, la divulgación y la destrucción, entre muchas otras.
Un firewall funciona como una serie de capas que componen una estrategia de defensa en sentido de profundidad; también es como un sistema de filtros que identifica y categoriza cada elemento del flujo de datos para impedir el acceso de los no deseados.
Por lo que el sistema analiza todo el tráfico de la red en lugar de responder ante un ataque ya iniciado.

La función básica del firewall en la seguridad de la red es controlar el tráfico que pasa entre dos redes y bloquear todo lo que no esté explícitamente permitido.

De esta manera el firewall previene muchos ataques. También impiden el acceso remoto a estaciones de trabajo y servidores empresariales, al aislar una red y el internet en general, como un muro de contención.

- La red inalámbrica permitirá a los usuarios permanentes, así como visitantes obtener servicios corporativos o conexiones transitorias controladas para no entorpecer las tareas internas de la entidad.

3. **SISTEMAS DE PROCESAMIENTO, INFORMACION Y ALMACENAMIENTO:** Como tercera fase se identificaron los sistemas de procesamiento y almacenamiento encontrando que no existen estos elementos dentro de la institución.

Al no poseer estos elementos dentro del plan de mejoras para el manejo de la información se propone: El uso de mínimo un servidor para la autenticación de los usuarios en el sistema por medio de la construcción de un controlador de dominio. Este controlador permitirá emitir las políticas para ejercer autoridad dentro de la red autorizando o des-autorizando accesos con privilegios a los diferentes servicios dentro de la entidad.

¿Porque usar un controlador de dominio?
Para entender echemos un vistazo a la primera palabra, "dominio". Un dominio se relaciona con una red que aloja varias computadoras y dispositivos. Piense en el dominio como un concentrador maestro al que están conectados todos los dispositivos y ese concentrador puede controlar cualquier dispositivo que sea parte de la red. Esto incluye cosas como:

- Ordenadores
- Laptops
- Impresoras
- Cámaras de seguridad
- Servidores
- Y otros dispositivos

Todos los componentes conectados están registrados en una base de datos central ubicada en el controlador de dominio.

Cuando vea el término "controlador de dominio", también verá un término asociado, "Active Directory (AD)", que es un servicio de directorio de Microsoft para sus redes de dominio de Windows. Un servidor que ejecuta los Servicios de dominio de Active Directory se conoce como controlador de dominio.

Características

- Dar acceso solo a aquellos que lo necesitan
- Evite las infracciones de datos de "error del operador"
- La gestión centralizada reduce los costos
- Recursos informáticos compartidos

Para salvo guardar la información de primera instancia en el caso de requerir recuperación de datos por perdida en activos, virus, o ataques informáticos es requerido un sistema de almacenamiento NAS.

¿Porque una NAS?
El almacenamiento conectado en red, Network Attached Storage (NAS), es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador/ordenador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

4. **SISTEMAS DE PROTECCIÓN ELÉCTRICA Y ENFRIAMIENTO:** En la cuarta fase se identificaron los sistemas de suministro y protección eléctrica dentro de los cuales se encontró lo siguiente:
   - Sistema actual de energía primario suministrado por Emcali.
   - No existe sistema secundario eléctrico planta eléctrica.

- Dentro de las instalaciones no existe una red regulada de energía para salvo guardar los sistemas de cómputo de usuarios y de Core.
- Se encontró un sobre dimensionamiento de la planta operativa con un crecimiento superior al 50% en personal al igual que en equipos de cómputo.
- Los sistemas actuales de energía no poseen filtros para prevenir las sobre tensiones eventuales que existen en sistemas eléctricos.
- Los sistemas de no están estructurados ni automatizados para regular los consumos excesivos.
- No existen elementos de protección para equipos de cómputo tales como UPS.
- No se encontró un cuarto técnico con las condiciones mínimas de seguridad, enfriamiento y potencia para sostener los sistemas críticos de la entidad.
- No existe sistema de protección a puesta tierra.

INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN **PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI** **PROCESO GESTIÓN ADMINISTRATIVA**	CODIGO	PA-PL-242-004
		VERSIÓN	2
		APROBADO	10/MAR/2021

DOFA

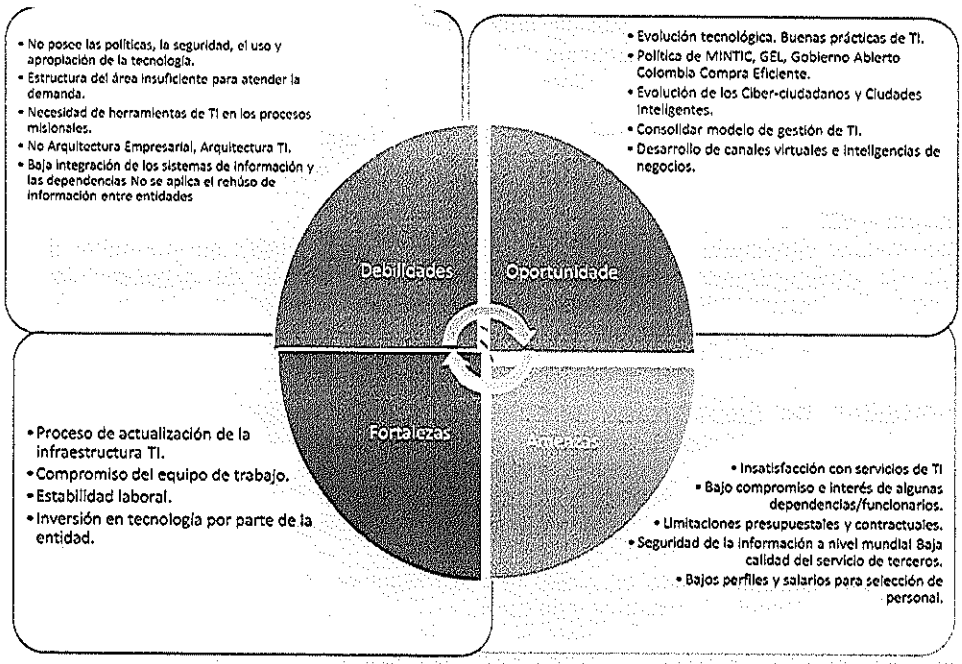


Imagen 2: matriz DOFA del componente tecnológico INDERVALLE

De acuerdo con el levantamiento de la información y el análisis realizado, se identifican los aspectos más relevantes agrupándolos en la matriz para su evaluación como parte de la metodología.

Debilidades
No posee las políticas, la seguridad, el uso y apropiación de la tecnología.
Estructura del área insuficiente para atender la demanda.
Necesidad de herramientas de TI en los procesos misionales.
No Arquitectura Empresarial, Arquitectura TI.
Baja integración de los sistemas de información y las dependencias No se aplica el rehúso de información entre entidades
Oportunidades
Evolución tecnológica. Buenas prácticas de TI.
Política de MINTIC, GEL, Gobierno Abierto Colombia Compra Eficiente.
Evolución de los Ciber-ciudadanos y Ciudades Inteligentes.
Consolidar modelo de gestión de TI.
Desarrollo de canales virtuales e inteligencias de negocios.
Amenazas
Insatisfacción con servicios de TI
Bajo compromiso e interés de algunas dependencias/funcionarios.

Limitaciones presupuestales y contractuales.
Seguridad de la información a nivel mundial Baja calidad del servicio de terceros.
Bajos perfiles y salarios para selección de personal.
Fortalezas
Proceso de actualización de la infraestructura TI.
Compromiso del equipo de trabajo.
Estabilidad laboral.
Inversión en tecnología por parte de la entidad.

8. ESTRATEGIAS PLAN ESTRATÉGICO DE TECNOLOGÍAS, PETI

Las estrategias del PETI, se basa en dos aspectos relevantes para la entidad la generación de valor para los usuarios y la gestión de TIC, para esto se utilizan dos componentes en construcción como lo son la Política de seguridad de la Información que se encuentra en el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamientos de Riesgos. Se muestra el listado de vulnerabilidades y las acciones para mitigar el impacto de los riesgos establecidos en el plan de tratamiento.

8.1 Riesgos

No.	VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	CALIFICACIÓN	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN	MITIGACIÓN DEL RIESGO	VIGENCIA DE CUMPLIMIENTO
1	Afectación de activos de información y activos informáticos	Desconocimiento de las políticas y normas de seguridad de la información.	No socialización y No capacitación de los políticas y normas de seguridad.	Acciones no adecuadas en el tratamiento de los activos de información o informáticos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Implementar la política de seguridad de la información según el plan de seguridad y privacidad de la información	Vigencia 2020
2	Fallas eléctricas	La entidad no cuenta con una UPS en caso de caida de voltajes y corte del fluido eléctrico	No cuenta con el plan de continuidad del negocio	Pérdida total de información sensible, deterioro en los equipos de computo	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Adquirir una UPS centralizada que brinde respaldo eléctrico a la entidad	Vigencia 2020
3	Perdida y deterioro de los equipos de comunicaciones	La entidad no cuenta no tiene un Centro de datos con las condiciones mínimas de acuerdo a la norma TIA 942	Perdida, Hurto o Daño físico de los equipos de comunicaciones debido a la exposición de los equipos	Interrupción de las actividades, Pérdida de la información	* Riesgo Tecnológico * Riesgo en Servicio	60	Probable	Riesgo Mayor	Diseñar un centro de datos donde se salvaguarden los equipos de comunicaciones y cuente con en contra de acceso para garantizar su custodia	Vigencia 2020
4	Pérdida de Información	Falta de protección contra malware, software no deseado y virus	No se cuenta con un antivirus de red que permita monitorear los posibles sucesos de infección	Pérdida total de información sensible, Robo de información, * Pérdida de tiempo operacional, Pérdida de oportunidad, Costo financiero Imagen, reputación y buen nombre.	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	100	Casi seguro	Riesgo Alto	Adquirir un software antivirus, licenciado con monitoreo de Red	Vigencia 2020
5	Incumplimiento de las actividades de seguridad de la información.	La entidad debe capacitar a los funcionarios en temas de compromisos y de las políticas de seguridad de la información	Se debe implementar el plan de capacitación de seguridad de la información	Incumplimiento del plan de seguridad y privacidad y falta de capacitación y transferencia de conocimiento en el tema	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Capacitar y asesorarse profesionalmente en el tema de implementación de la política de seguridad de la información	Vigencia 2020
6	Atrasos en la entrega de información	La entidad debe articular el sistema de gestión documental con el sistema de PQRS	Unificar los canales por los cuales la entidad recibe los PQRS	Se debe implementar un módulo o interfaz entre el SIDOCS y la página web	Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Implementar la interfaz de ventanilla única integrado al sistema de PQRS	Vigencia 2020

INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN **PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI** **PROCESO GESTIÓN ADMINISTRATIVA**	CODIGO	PA-PL-242-004
		VERSIÓN	2
		APROBADO	10/MAR/2021

7	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Aplicar el plan de mantenimiento correctivo de la entidad	Incumplimiento en el mantenimiento del sistema de información.	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio	60	Probable	Riesgo Alto	Cumplir el plan de mantenimiento preventivo y correctivo para los equipos de cómputo de la entidad	Vigencia 2020
8	Ausencia de esquemas de reemplazo periódico	la entidad no mide los niveles de obsolescencia de los equipos para así poder dar de baja o reemplazarlos	Destrucción de equipos o medios.	Se debe de contar con buenos equipos al igual que los no funcionales darles un destino final adecuado preservando la confidencialidad de la información	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	40	Posible	Riesgo Moderado	Crear el plan de disposición final de residuos tecnológicos	Vigencia 2020
9	Susceptibilidad a la humedad, el polvo y la suciedad	Aplicar el plan de mantenimiento correctivo de la entidad	Polvo, corrosión y congelamiento	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio	60	Probable	Riesgo Alto	Cumplir el plan de mantenimiento preventivo y correctivo para los equipos de cómputo de la entidad	Vigencia 2020
10	Ausencia de un eficiente control de cambios en la configuración	La entidad no cuenta con un software monitor para gestionar el control de cambios de los equipos.	Error en el uso	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio	60	Probable	Riesgo Mayor	Diseñar un Software de gestión de activos de información para el control de cambios en la configuración tanto como el control original de los equipos como su reparación por mantenimiento correctivo	Vigencia 2020
11	Susceptibilidad a las variaciones de voltaje	La entidad no cuenta con una UPS en caso de caída de voltajes y corte del fluido eléctrico	Pérdida del suministro de energía	Pérdida total de información sensible, deterioro en los equipos de computo	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Adquirir una UPS centralizado que brinde respaldo eléctrico a la entidad	Vigencia 2020
12	Susceptibilidad a las variaciones de temperatura	La entidad debe contar con el plan de gestión de incidentes donde se establezcan los lineamientos en caso de un desastre natural	Fenómenos meteorológicos	Pérdida total de información sensible, deterioro en los equipos de computo	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo Financiero	60	Probable	Riesgo Alto	Garantizar las condiciones ideales para los equipos con mantenimientos preventivos y un centro de datos para los equipos de comunicaciones	Vigencia 2020
13	Almacenamiento sin protección	Falta de protección contra malware, software no deseado y virus	Hurtos medios o documentos.	Pérdida total de información sensible, Robo de información, * Pérdida de tiempo operacional, Pérdida de oportunidad, Costo financiero Imagen, reputación y buen nombre.	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	100	Casi Seguro	Riesgo Alto	Adquirir un software antivirus, licenciado con monitoreo de Red	Vigencia 2020
14	Falta de cuidado en la disposición final	La entidad no cuenta con la política de disposición final de residuos tecnológicos	Hurtos medios o documentos.	perdida de información o hurto en discos duros, memorias USB, medios ópticos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	40	Posible	Riesgo Moderado	Crear el plan de disposición final de residuos tecnológicos	Vigencia 2020
15	Ausencia o insuficiencia de pruebas de software	La entidad no cuenta con los ambientes de prueba y producción de la página web con el fin de realizar las pruebas de software.	Abuso de los derechos	Accesos no autorizados, perdida de información por seguridad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo Financiero	60	Probable	Riesgo Mayor	Realizar pruebas de SQL inyección, y crear un sistema de auditoria y acceso a la web	Vigencia 2020
16	Defectos bien conocidos en el software	la entidad no documenta los errores y fallas de los aplicativos y páginas web	Abuso de los derechos	No hay un control de cambios y actualizaciones de software	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	40	Posible	Riesgo Moderado	Diseñar un control de cambios y mantenimiento de software con el fin de garantizar la documentación de las fallas y reparaciones	Vigencia 2020
17	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Algunos equipos están configurados para bloquear el usuario por inactividad	Abuso de los derechos	Intento de acceso no autorizado para hurto o fraude	* Riesgo Tecnológico * Riesgo en Servicio	40	Posible	Riesgo Moderado	Implementar un Directorio activo para configurar los inicios de sección en la entidad	Vigencia 2020
18	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	La entidad no cuenta con la política de disposición final de residuos tecnológicos	Abuso de los derechos	perdida de información o hurto en discos duros, memorias USB, medios ópticos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	40	Posible	Riesgo Moderado	Crear el plan de disposición final de residuos tecnológicos	Vigencia 2020
19	Ausencias de pistas de auditoria	la entidad cuenta con Log de auditoria pero deben mejorarse las políticas de contraseñas y usabilidad de los equipos	Abuso de los derechos	Los usuarios pueden facilitar sus contraseñas y usuarios para acceder a información sensible o reservada	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	60	Muy Probable	Riesgo Mayor	Realizar un plan de seguimiento a los Log de acceso de la entidad	Vigencia 2020

20	Asignación errada de los derechos de acceso	La entidad cuenta con un registro de asignación de usuarios con sus respectivos privilegios	Abuso de los derechos	Los usuarios puedan usar funciones a las cuales no están autorizados o realizar modificaciones a información reservada	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	60	Muy Probable	Riesgo Mayor	Realizar y actualizar el registro de asignación de usuarios y privilegios en los aplicativos de la entidad	Vigencia 2020
21	Ausencia de documentación	Los desarrollos internos como la página web debe de tener su respectiva documentación diagrama de casos de uso, diagrama de transacionalidad, la ayuda entre otros	Error en el uso	Informa el desarrollo el tipo de lenguaje utilizado e informa la funcionalidad del sitio web	* Riesgo de la Información	40	Posible	Riesgo Moderado	Realizar la respectiva documentación de los desarrollos internos, pagina web	Vigencia 2020
22	Gestión deficiente de las contraseñas	la entidad cuenta con Log de auditoria pero deben mejorarse las políticas de contraseñas y usabilidad de los equipos	Falsificación de derechos	No hay un politica clara del uso efectivo de contraseñas	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	60	Muy Probable	Riesgo Mayor	Se debe establecer la política de gestión de contraseñas y asignación de usuarios	Vigencia 2020
23	Descarga y uso no controlado de software	Se debe controlar la instalación de software no permitido o no licenciado	Manipulación con software	No hay control en la instalación de software no licenciado y se incumple con los derechos de autor	* Riesgo Tecnológico * Riesgo de la Información	60	Muy Probable	Riesgo Mayor	Se debe bloquear todo tipo de instalación de software que no cumpla con las políticas de seguridad y que cumpla con los requisitos de licenciamiento	Vigencia 2020
24	Ausencia de copias de respaldo	La entidad cuenta con un servicio de disco duro en la nube	Manipulación con software	Se debe establecer una política copias de seguridad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Crear la política de copias de seguridad e implementarla en la entidad	Vigencia 2020
25	Ausencia de protección física de la edificación, puertas y ventanas	La entidad cuenta con un sistema de monitoreo cerrado	Hurto de medios o documentos	se debe ampliar la cantidad de dispositivos para proteger más áreas en la entidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	20	Improbable	Riesgo Menor	Se debe ampliar la cantidad de dispositivos de grabación y además implementar este tipo soluciones a las otras sedes de la entidad	Vigencia 2020
26	Ausencia del personal	La entidad el personal de sistemas es limitado y debe capacitarse en seguridad de la información	Incumplimiento en la disponibilidad del personal	Desconocimiento de la seguridad y personal lo que genera incumplimiento del plan de seguridad y privacidad y falta de capacitación y transferencia de conocimiento en el tema	* Riesgo Tecnológico * Riesgo en Servicio	40	Poco Probable	Riesgo Alto	Se debe contratar asesoría en seguridad de la información y capacitación al personal existente para la implementación de la política	Vigencia 2020
27	Entrenamiento insuficiente en seguridad	La entidad no capacita a los funcionarios y contratistas en seguridad de la información	Error en el uso	Desconocimiento de la seguridad y personal lo que genera incumplimiento del plan de seguridad y privacidad y falta de capacitación y transferencia de conocimiento en el tema	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se debe capacitar a todo el personal en seguridad de la información	Vigencia 2020
28	Falta de conciencia acerca de la seguridad	Los funcionarios desconocen la importancia del sistema de gestión de seguridad de la información	Error en el uso	Los usuarios incumplen las políticas de seguridad por desconocimiento	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se debe capacitar a todo el personal en seguridad de la información	Vigencia 2020
29	Ausencia de mecanismos de monitoreo	La entidad no cuenta con estrategias de control de datos y monitoreo a los sistemas sensibles	Procesamiento ilegal de los datos	Los sistemas de información no cuentan con Log de auditoria y si los tienen no se los realiza análisis de ellos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	60	Muy Probable	Riesgo Alto	Se deben de crear políticas de acceso y monitorear los ingresos a los aplicativos	Vigencia 2020
30	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	La entidad cuenta con un sistema de monitoreo cerrado	Accesos no autorizados	se debe ampliar la cantidad de dispositivos para proteger más áreas en la entidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	20	Improbable	Riesgo Menor	Se debe ampliar la cantidad de dispositivos de grabación y además implementar este tipo soluciones a las otras sedes de la entidad	Vigencia 2020
31	Ubicación en área susceptible de inundación	La entidad debe garantizar el mantenimiento constante de acueductos y alcantarillas en las sedes	Fenómenos metoorológicos y naturales	Pérdida total de información sensible, deterioro en los equipos de computo	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo Financiero	60	Probable	Riesgo Alto	Garantizar las condiciones idoneas en caso de desastres naturales poseer la continuidad del negocio	Vigencia 2020

INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN **PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI** **PROCESO GESTIÓN ADMINISTRATIVA**	CODIGO	PA-PL-242-004
		VERSIÓN	2
		APROBADO	10/MAR/2021

	Ausencia de procedimiento formal para el registro y retiro de usuarios	la entidad no cuenta un software para la política de ingreso y salida de usuarios	Abuso de los derechos	perdida de información al retirarse de la entidad información sensible y logos e información que puede ser usada en beneficio propio	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se deben de crear un software para las políticas de ingreso y salida de usuarios así como la entrega de la información en	Vigencia 2020
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Se debe mejorar la clausulas de seguridad de información en cuanto a la manipulación de la información	Abuso de los derechos	perdida de información sensible al final del contrato o abuso de confianza	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	60	Probable	Riesgo Alto	Se debe implementar el acuerdo de confidencialidad de la información con los contratistas	Vigencia 2020
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	La entidad no cuenta con estrategias de control de datos y monitoreo a los sistemas sensibles	Abuso de los derechos	Los sistemas de información no cuentan con Log de auditoria y si los tienen no se les realiza análisis de ellos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se deben de crear políticas de acceso y monitorear los ingresos a los aplicativos	Vigencia 2020
	Ausencia de auditorias	La entidad cuenta con auditorias de los entes de control, pero debe realizar los planes de acción respectivos a los hallazgos	Abuso de los derechos	No cumplir con las acciones de mejoras implantadas y contraer sanciones por incumplimiento	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	20	Improbable	Riesgo Menor	Se deben crear un mecanismo de revisión al plan de mejoramiento posterior a cada auditoria	Vigencia 2020
	Ausencia de procedimientos de identificación y valoración de riesgos	La entidad no cuenta con el procedimiento de gestión de riesgos	Abuso de los derechos	El nivel de que ocurran los riesgos es alto debido a que no existen un control y mitigación de los mismos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Aplicar la metodología y elementos planteados en este plan de gestión de Riesgos	Vigencia 2020
	Ausencia de reportes de fallas en los registros de administradores y operadores	No hay un Software o bitácora de los incidentes de los proveedores de servicio	Abuso de los derechos	Incidencias repetitivas y no soluciones oportunas a los daños frecuentes	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Implementar un software que los permitan monitorear las incidencias por los proveedores	Vigencia 2020
	Respuesta inadecuada de mantenimiento del servicio	No existe seguimiento a los mantenimientos por servicios	Incumplimiento en el mantenimiento del sistema de información	Incidencias repetitivas y no soluciones oportunas a los daños frecuentes	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Establecer los formatos que les permitan monitorear las incidencias por los proveedores	Vigencia 2020
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	la entidad no existe análisis los servicios prestados y los acuerdo que se pactan entre las entidades	Incumplimiento en el mantenimiento del sistema de información	Incumplimiento de los acuerdos por parte de los proveedores del servicio	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Analizar y verificar los ANS ofrecidos por los operadores de servicio para garantizar la continuidad del negocio	Vigencia 2020
	Ausencia de procedimientos de control de cambios	La entidad no cuenta con un formato de control de cambios o actualizaciones a los sistemas de información	Incumplimiento en el mantenimiento del sistema de información	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Diseñar los formatos de control de cambio de los aplicativos	Vigencia 2020
	Ausencia de procedimiento formal para la documentación del MSPI	La entidad no cuenta con la herramienta debido a que se encuentra en construcción la política	Corrupción de datos	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Implementar el Modelo de Seguridad y Privacidad de la Información como herramienta de control y monitoreo	Vigencia 2020
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	La entidad no cuenta con la herramienta debido a que se encuentra en construcción la política	Corrupción de datos	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Implementar el Modelo de Seguridad y Privacidad de la Información como herramienta de control y monitoreo	Vigencia 2020
	Ausencia de procedimiento formal para la autorización de la información disponible al público	La entidad debe establecer el mecanismo para suministrar información a la usuarios	Datos provenientes de fuentes no confiables	La información pública no se encuentra en datos.gov.co	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	La entidad debe actualizar la información publicada en datos.gov.co	Vigencia 2020
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	La entidad no cuenta con el comité establecido de la seguridad de la información	Negación de acciones	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se debe crear el comité de seguridad de la información	Vigencia 2020

INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN **PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI** **PROCESO GESTIÓN ADMINISTRATIVA**	CODIGO	PA-PL-242-004
		VERSIÓN	2
		APROBADO	10/MAR/2021

	Ausencia de planes de continuidad	La entidad no cuenta con plan de continuidad ni eléctrico, ni políticas de copias de seguridad interna o externa	Falla del equipo	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Diseñar el plan de continuidad del negocio y el plan de recuperación de desastres tecnológicos	Vigencia 2020
	Ausencia de políticas sobre el uso de correo electrónico	La entidad cuenta con su correo corporativo institucional pero deben establecer políticas para su uso y apropiación	Error en el uso	Perdida de información por ataque o infección por virus o malware	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	La entidad debe formular políticas de usabilidad del correo institucional	Vigencia 2020
	Ausencia de registros en bitácoras	La entidad no registra los incidentes en bitácoras o controles de cambio	Error en el uso	Perdida incalculable de información sensible	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Es necesario implementar bitácoras en los procesos para medir el impacto y la gestión del área	Vigencia 2020
	Ausencia de procedimientos para el manejo de información clasificada	La entidad en sus procedimientos no muestra la clasificación de la información	Error en el uso	La información se fuga de forma fácil al no estar clasificada	* Riesgo en Servicio * Riesgo de la Información	100	Casi Seguro	Riesgo Alto	Se debe clasificar la información y establecer el uso apropiado de la misma mediante un procedimiento.	Vigencia 2020
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	La entidad debe mejorar las cláusulas contractuales donde se evidencien las responsabilidad en la seguridad de la información	Error en el uso	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Incluir los acuerdos de confidencialidad y privacidad en las etapas contractuales	Vigencia 2020
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	La entidad debe mejorar las cláusulas contractuales donde se evidencien las responsabilidad en la seguridad de la información	Hurto de equipo	Incumplimiento del plan de seguridad y privacidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Incluir los acuerdos de confidencialidad y privacidad en las etapas contractuales	Vigencia 2020
	Ausencia de política formal sobre la utilización de computadores portátiles	La entidad no cuenta con una política de uso de equipos portátiles y trabajo mediante conexión remota	Hurto de equipo	Fuga incontrolada de información por equipos portatiles de los contratistas	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	100	Casi Seguro	Riesgo Alto	Diseñar la política de uso de equipos portátiles tanto de contratistas como de externos	Vigencia 2020
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	La entidad cuenta con una sede alterna llamada reten forestal la cual debe hacer seguimiento de los activos de información y control del mismo	Hurto de equipo	Perdida de información y monitoreo de la información generada y manipulada	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	100	Casi Seguro	Riesgo Alto	Crear aplicaciones que permitan centralizar la información en la nube y controlar el acceso remoto	Vigencia 2020
	Ausencia de política sobre limpieza de escritorio y pantalla	La entidad no cuenta con la política de pantallas limpias	Hurto de medios o documentos	La información se encuentra expuesta en el escritorio y de fácil acceso a los usuarios	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	100	Casi Seguro	Riesgo Alto	Crear y aplicar el uso de pantallas limpias y manejo adecuado de la información	Vigencia 2020
	Ausencia de autorización de los recursos de procesamiento de información	Los procedimientos de autorización de recursos de información no cuentan con un procedimiento establecido	Hurto de medios o documentos	Los usuarios deben de notificar los movimientos de información sensible o reservada de la entidad	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se deben de establecer procedimientos para el manejo de la información sensible o reserva.	Vigencia 2020
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	La entidad no ha realizado ejercicios de análisis de brechas de seguridad	Hurto de medios o documentos	La información se encuentra expuesta en la red de la entidad y puede ser accesible desde cualquier punto interno	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se deben de realizar pruebas de seguridad y verificar cuales son los activos de información a proteger	Vigencia 2020
	Ausencia de revisiones regulares por parte de la gerencia	La gerencia ha evidenciado las debilidades en el área por esta razón dispone la realización y justificación de este plan de gestión de riesgos tecnológicos	Uso no autorizado de equipo	La gerencia utilize los hallazgos de la auditoria de la contraloría para iniciar medidas correctivas	* Riesgo en Servicio * Riesgo de la Información	40	Posible	Riesgo Moderado	La gerencia debe implementar los plan de seguridad y privacidad y el plan de tratamiento para mejorar en los aspectos tecnológicos de la entidad	Vigencia 2020
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	La entidad no cuenta con seguimientos de los incidentes e informes periódicos de gestión del área de tecnología	Uso no autorizado de equipo	La entidad debe mejorar el seguimiento a los informes de gestión tecnológica	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información	80	Muy Probable	Riesgo Alto	Se debe establecer la política de seguimiento y control a los informes tecnológicos de la entidad	Vigencia 2020

	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Los empleados contratistas no cuentan con licenciamiento en sus aplicativos para realizar los trabajos de la entidad	Uso de software falsificado o copiado	La entidad cuenta con software sin licenciamiento	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información *Riesgo financiero	100	Casi Seguro	Riesgo Alto	Se debe establecer el uso del software legal por parte de los contratistas	Vigencia 2020

8.2 Políticas de la seguridad de la información

De los controles principales se recomienda implementar el componente de las políticas de:

8.2.1 Políticas de gestión de comunicaciones y operaciones

- **Acceso a información sobre proyectos de la Entidad:** Solamente personas autorizadas pueden tener acceso a datos confidenciales sobre proyectos de propiedad de la Entidad o administrados por sus ejecutivos.
- **Activación de los Planes de Continuidad:** Cada plan de continuidad del negocio debería especificar claramente las condiciones para su activación, los procedimientos de emergencia a llevar a cabo, los procedimientos de respaldo que permitirán operar, los procedimientos de reanudación en condiciones de normalidad, así como las personas responsables de ejecutar cada etapa del plan.
- **Análisis de incidentes de Seguridad de la Información ocasionados por fallas de sistemas:** Los incidentes de seguridad de la información originados por fallas de hardware o software deben investigarse de manera apropiada por especialistas.
- **Análisis y especificación de los requisitos de seguridad:** Todo desarrollo de software, dentro o fuera de la Entidad, debe contar con un sustento técnico-económico, un presupuesto adecuado, una justificación basada en requerimientos de usuario previamente descritos, analizados y aprobados al nivel adecuado por el encargado del área de Sistemas y del área usuaria. Así mismo debe existir un compromiso de disponer de los recursos necesarios para solventar el proyecto de inicio a fin. La aprobación final del proyecto debe ser por parte de la Dirección Administrativa.
- **Certeza de orígenes de archivos:** Los archivos electrónicos recibidos de remitentes desconocidos deben ser eliminados sin ser abiertos
- **Comprobación de exactitud y validez de documentos:** Se debe confirmar la validez e integridad de documentos, especialmente aquellos que comprometen u obligan a la Entidad.
- **Confidencialidad de los incidentes de Seguridad de la Información:** La información relacionada a incidentes de seguridad de la información sólo puede ser divulgada entre personas autorizadas.
- **Configuración de acceso a Internet:** El personal encargado de configurar el acceso a Internet debe asegurarse que la Red de la Entidad tenga la debida protección. Como mínimo se debe instalar un firewall debidamente configurado.
- **Continuidad del negocio y análisis de impactos:** Los usuarios dueños de los sistemas de información, conjuntamente con los responsables técnicos de su manejo e identificarán los eventos de riesgo potencialmente causantes de interrupciones a procesos y/o servicios.
- **Control de Cambios Operacionales:** Los cambios operacionales deben probarse exhaustivamente y ser aprobados formalmente antes de ser puestos en producción.
- **Control de distribución de información:** Los datos e información deben protegerse mediante controles técnicos y administrativos a fin de asegurarse que están disponibles sólo para personas autorizadas.
- **Cronograma de Copias de Seguridad:** Los cronogramas de estas operaciones automatizadas que programa el personal de apoyo técnico deben planearse y contar con la autorización del encargado del área de Sistemas.

- **Defensa contra ataques internos intencionales:** Los estándares de control de acceso y de clasificación de datos deben ser revisados y actualizados periódicamente para reducir la incidencia y la posibilidad de ataques internos.
- **Defensa contra virus informáticos:** Todas los PCs y servidores de la Entidad deben tener instalado un software antivirus actualizado diariamente. Igualmente, se deben escanear regularmente todos los equipos. El software antivirus debe adquirirse de un proveedor reconocido, que tenga soporte técnico adecuado.
- **Dependencias entre documentos y archivos:** Los documentos altamente sensibles o críticos no deben depender de la disponibilidad o integridad de archivos de datos sobre los que el autor no tenga control. Los documentos e informes importantes deben ser autónomos y contener toda la información necesaria.
- **Desarrollo y mantenimiento de sitios Web:** Solamente personal debidamente calificado y autorizado participará en el desarrollo y mantenimiento de sitios Web de la Entidad.
- **Desarrollo y mantenimiento de software:** Las especificaciones técnicas y funcionales para el desarrollo y mantenimiento de software deben contemplar formalmente los requerimientos de seguridad, incluyendo los controles técnicos de acceso, la asignación restringida de privilegios y otros requisitos que resulten convenientes para dicha aplicación.
- **Descargar archivos e Información de Internet:** Se debe tener mucho cuidado al descargar información y archivos de Internet a fin de evitar el ingreso de código malicioso, así como la descarga de material no apropiado.
- **Documentación de procedimientos operativos:** Los procedimientos operativos deben especificar las instrucciones detalladas para la ejecución de cada tarea, incluyendo las actividades de administración de sistemas. Dichos procedimientos deben estar documentados formalmente.
- **Documentación de sistemas:** Todos los sistemas deben tener documentación completa y actualizada. Ningún sistema debe pasar a producción si no tiene la documentación de soporte disponible.
- **Elaboración de bases de datos:** Antes de poner una base de datos en producción, se deben realizar pruebas exhaustivas de su funcionamiento, tanto a nivel lógico de su estructura, como de su eficiencia en un ambiente de producción.
- **Eliminación de archivos temporales (tmp):** Los archivos temporales en las computadoras de usuarios deben ser eliminados con regularidad para prevenir su posible mal uso por usuarios no autorizados.
- **Eliminación segura de documentos:** Todos los documentos de naturaleza confidencial deben ser destruidos cuando ya no se requieren. El dueño del documento debe autorizar o realizar esta destrucción.
- **Eliminación de Software:** Sólo se debe eliminar un programa de software cuando se haya decidido que dicho programa ya no es necesario y que no se necesita tener acceso a sus archivos de datos mediante dicho programa.
- **Envío de información a terceros:** Antes de enviar información a terceros, se debe verificar que el receptor está autorizado a recibir dicha información y que las medidas adoptadas por los receptores aseguran la confidencialidad e integridad de la información que se envía. Se prohíbe facilitar reportes impresos, documentos, acceso a computadores personales e información propia del INDERVALLE a personas ajenas a la Entidad, sin autorización.
- **Estándares de control de acceso:** Los estándares de control de acceso de los sistemas de información deben establecerse de manera que prevengan ingresos de usuarios no autorizados y a la vez proporcionen acceso inmediato según los requerimientos de la Entidad.

- **Estructura de carpetas y datos para usuarios:** Las estructuras de carpetas de datos de la red compartidos por los usuarios deben ser definidas por el encargado del área de Sistemas y los usuarios deben seguir dicha estructura. Las restricciones de acceso se deben aplicar para evitar o prevenir el acceso no autorizado.
- **Evidencias del evento de riesgo:** Es indispensable recolectar evidencias después de la ocurrencia de eventos de riesgo sobre la seguridad de la información.
- **Fotocopiado de información confidencial:** Los trabajadores deben conocer los riesgos de brechas de confidencialidad durante el fotocopiado/duplicación de documentos. Sólo se debe duplicar documentos confidenciales con la debida autorización del dueño del documento.
- **Gestión de redes:** Los administradores de redes deberán implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadoras, así como la integridad de la red y protección de los servicios conectados contra accesos no autorizados.
- **Iniciativa para el Plan de Continuidad del Negocio:** La Dirección Administrativa o en su ausencia del encargado del área de Sistemas se debe tener la iniciativa para iniciar la ejecución del Plan de Continuidad del Negocio.
- **Instalación usuarios de software adicional:** Está prohibido instalar software no autorizado en las computadoras de la Entidad, tales como protectores de pantalla, software demostrativo, manejadores de música, video, mensajería instantánea, juegos, protectores de pantalla, aplicativos particulares (software con licencia adquirido por el usuario para uso doméstico), aplicativos recibidos por la red (correo electrónico, internet), aplicativos entregados en calidad de prueba; salvo autorización del encargado del área de Sistemas, para fines de evaluación y pruebas preliminares.
- **Integridad de material de evidencia:** La integridad de todo material de evidencia debe ser protegida. Las copias deben ser supervisadas por personal confiable y se debe registrar la información de cuando y donde fue ejecutado el proceso de copia, quien realizo dicha actividad, y que herramientas y programas se utilizaron.
- **Interfaz de software aplicativo:** El desarrollo de interfaz de sistemas es una tarea altamente especializada y por lo tanto sólo debe ser realizada por profesionales con la debida calificación y experiencia comprobada en el tema. Debe considerar sobremanera los aspectos de seguridad de los sistemas que son conectados y de las plataformas que intervienen.
- **Mantenimiento y concientización:** Todo plan de continuidad debe tener un calendario de mantenimiento de pruebas del plan, así como prever actividades de concientización y capacitación diseñadas para asegurar que los procesos sean eficaces.
- **Mantenimiento y reevaluación del Plan de Continuidad del Negocio:** El Plan de Continuidad del Negocio debe ser continuamente actualizado para reflejar los cambios en los recursos, procesos y servicios de la Entidad.
- **Medidas y controles contra software malicioso:** Todos los recursos activos de tratamiento de información: infraestructura de red, software base y de aplicación, deben configurarse y protegerse adecuadamente contra ataques físicos e intrusión.
- **Minimización de impacto de ataques informáticos:** Se deben elaborar planes para minimizar los daños por posibles ataques informáticos, los que deberán ser mantenidos y probados periódicamente para asegurar su eficacia y que los tiempos de recuperación sean razonables.
- **Monitoreo de los Logs de operaciones:** Los registros de log operacional deben ser revisados periódicamente por personal calificado y las discrepancias con los procedimientos operacionales deben ser comunicadas al usuario propietario de información y al encargado del área de Sistemas
- **Paralelo de sistemas:** Los procedimientos de prueba de sistemas deben considerar un período de funcionamiento paralelo antes que el sistema nuevo o mejorado sea aceptado para su uso en

producción. Los resultados del paralelo no deben revelar problemas o dificultades diferentes a los ya vistos durante la prueba de aceptación de usuario.

- **Plan de recuperación de desastres:** Los usuarios dueños de cada sistema de información deben asegurarse que disponen de planes de recuperación de desastres, documentados, probados y en funcionamiento.
- **Planeamiento de capacidad y prueba de nuevos sistemas:** Para las pruebas de nuevos sistemas se deben aplicar criterios de capacidad, carga máxima y prueba de stress. Debe demostrarse que sus niveles de rendimiento y resistencia cumplen o exceden las necesidades o requisitos técnicos de la Entidad.
- **Probar debilidades:** Se deben probar técnicamente las debilidades del sistema (Ethical Hacking) sin producir mal uso, ni ocasionar daños al mismo o al servicio de información, ni incurrir en responsabilidades legales para quien realiza la prueba. La gestión de la continuidad del negocio debe incorporarse en los procesos y estructura de la Entidad, asignando la responsabilidad de coordinación de este proceso a la oficina de Sistemas. El proceso de continuidad del negocio debe incluir la identificación y priorización de los procesos críticos y el impacto de las interrupciones. Los planes y procesos de continuidad así definidos deben probarse y actualizarse periódicamente.
- **Procedimiento del reporte:** Los procedimientos de reporte del cual deben tener conocimiento los empleados, contratistas y terceros, deben incluir: procesos de retroalimentación que aseguren que los eventos sean notificados; formulario de reporte, el cual apoya la acción del reporte y ayuda al encargado del reporte a recordar las acciones necesarias cuando se produce un evento.
- **Protección de documentos electrónicos con contraseñas** Se debe proteger la información confidencial usando, preferentemente, el control de acceso de la carpeta donde está situado el archivo correspondiente. No se recomienda el uso solamente de contraseñas para proteger documentos.
- **Protección contra ataques de negación de servicio (DoS):** Se deben tener listos planes de acción contra ataques de negación del servicio (DoS) los cuales deben ser mantenidos y probados periódicamente para asegurarse de su eficacia.
- **Prueba del Plan de Continuidad del Negocio:** El Plan de Continuidad del Negocio debe ser probado periódicamente para asegurarse que cada uno de los responsables de las diferentes acciones entienda correctamente la ejecución del Plan.
- **Recepción de correo no solicitado:** Se debe verificar la identidad y la autenticidad del remitente de cualquier mensaje de correo electrónico no solicitado antes de abrirlo.
- **Registro y reporte de fallas de equipos:** Toda falla de equipos (incluyendo daños) debe anotarse en un registro especialmente designado para tal fin por el personal encargado de su mantenimiento.
- **Registro y reporte de fallas de software:** Se debe registrar y reportar formalmente toda falla de software a los responsables de soporte de software.
- **Reporte de eventos y debilidades de la Seguridad de la Información:** El área de Sistemas debe establecer un procedimiento formal de reporte de eventos o incidentes de riesgos sobre la seguridad de la información que indique las respuestas y las acciones que deben ser tomadas.
- **Respaldo y recuperación de la información:** Es de alta prioridad generar copias de respaldo de archivos de datos (backup) de la Entidad y garantizar la capacidad de restaurarlos. El encargado del área de Sistemas será responsable de que la frecuencia de tales operaciones y que los procedimientos aplicados se adecuan a las necesidades de la Entidad.
- **Respuestas ante incidentes de Seguridad de la Información:** El encargado del área de Sistemas debe responder rápidamente a cualquier incidente de Seguridad de la Información, coordinando la recolección de información y sugiriendo medidas a tomar donde sea necesario.

- **Respuesta a incidentes de virus:** Se debe desarrollar una estrategia integral y procedimientos de actuación para hacer frente a los virus informáticos, lo cual incluirá procedimientos y responsabilidades de administración, capacitación en el uso de software antivirus y recuperación después de los ataques de virus.
- **Segregación de funciones:** Necesidad de control dual / segregación de funciones Donde quiera que un incidente de seguridad de la información pueda ocasionar daño material o financiero a la Entidad, debe emplearse técnicas de control dual y segregación de funciones para mejorar el control de procedimientos de seguridad.
- **Seguridad de la documentación de sistemas:** La documentación de sistemas es un requisito obligatorio para todo sistema de información de la Entidad. Dicha documentación debe mantenerse actualizada y disponible.
- **Seguridad de sistemas públicamente disponibles:** Se deben establecer controles en los sistemas públicamente disponibles de captura de información con la finalidad que la información confidencial se proteja durante su recojo y almacenamiento, y que el acceso a dicho sistema no permita accesos no autorizados a otras redes a las que está conectado el sistema.
- **Seguridad en el Envío de correo electrónico:** Se debe utilizar el correo electrónico solamente para fines relacionados con la Entidad. Antes de adjuntar archivos a un mensaje de e-mail se debe verificar que la clasificación de información de dicho archivo permite su envío al destinatario previsto y también. Previamente se debe escanear y verificar que no exista virus u otro código malicioso.
- **Seguridad en la Recepción de correo erróneo:** Los mensajes de correo electrónico no solicitado deben ser tratados con precaución y no ser respondidos.
- **Separación de los ambientes computacionales de desarrollo y de producción:** El encargado del área de Sistemas debe asegurarse que existe una segregación de funciones apropiada en todas las áreas encargadas de funciones de desarrollo, operaciones y administración de sistemas.
- **Tercerización de operaciones:** En el caso de tercerización de operaciones, se deben identificar los riesgos por anticipado e incorporar al contrato las medidas de seguridad apropiadas.
- **Transmisión e intercambio de información de banca virtual u otra confidencial:** Solamente se puede transmitir datos o información de banca virtual u otro tipo de información confidencial cuando la seguridad de los datos puede garantizarse razonablemente usando técnicas de encriptación.
- **Transporte de documentos confidenciales:** Las medidas de protección de la confidencialidad, integridad y disponibilidad en el transporte o transmisión de documentos confidenciales serán establecidas por los dueños de dichos documentos, quienes deberán asegurarse que tales medidas son las apropiadas.
- **Uso de buenas prácticas de gestión de información:** Todos los usuarios deben proteger la confidencialidad, integridad y disponibilidad de los archivos durante la creación, almacenamiento, modificación, copiado y borrado/eliminación de archivos de datos.
- **Uso de medios removibles de almacenamiento:** Solamente el personal autorizado a instalar o a modificar el software podrá utilizar medios removibles para transferir datos de la Entidad. Cualquier otra persona requerirá autorización expresa.
- **Uso de correo electrónico:** Está prohibido usar el correo electrónico para las labores ajenas a la Entidad. Se debe evitar el uso de lenguaje obsceno y/o abusivo. Si se reciben mensajes de cadenas recomendando que los distribuya a sus amigos, NO lo haga. Elimínelos sin abrirlos. Está prohibido el envío y distribución de mensajes desde el correo electrónico corporativo no relacionados con el desarrollo de las actividades de la Entidad. Cada empleado con acceso a Internet podrá utilizar su correo electrónico personal de forma razonable. Se deberá tener en

consideración que los mensajes enviados por el correo electrónico tendrán plena validez para todos los efectos, es decir serán considerados como documentos oficiales. Se deberá revisar los mensajes antes de enviarlos, verificando el destinatario y/o las listas de distribución, para asegurarse que todos los receptores del correo requieren conocer la información.

- **Uso de equipos de fax y fax-módems:** Sólo se puede enviar información confidencial por fax cuando no estén disponibles métodos más seguros de transmisión. El dueño de la información y el recipiente previsto debe estar avisado y autorizar las transmisiones por anticipado. Se debe comprobar cuidadosamente las direcciones de email y números de fax antes de enviar información, especialmente en los casos de información confidencial. La misma precaución debe aplicarse cuando existe la posibilidad que se divulguen las direcciones de E-mail u otra información de contacto.

9. MODELO DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN, TI

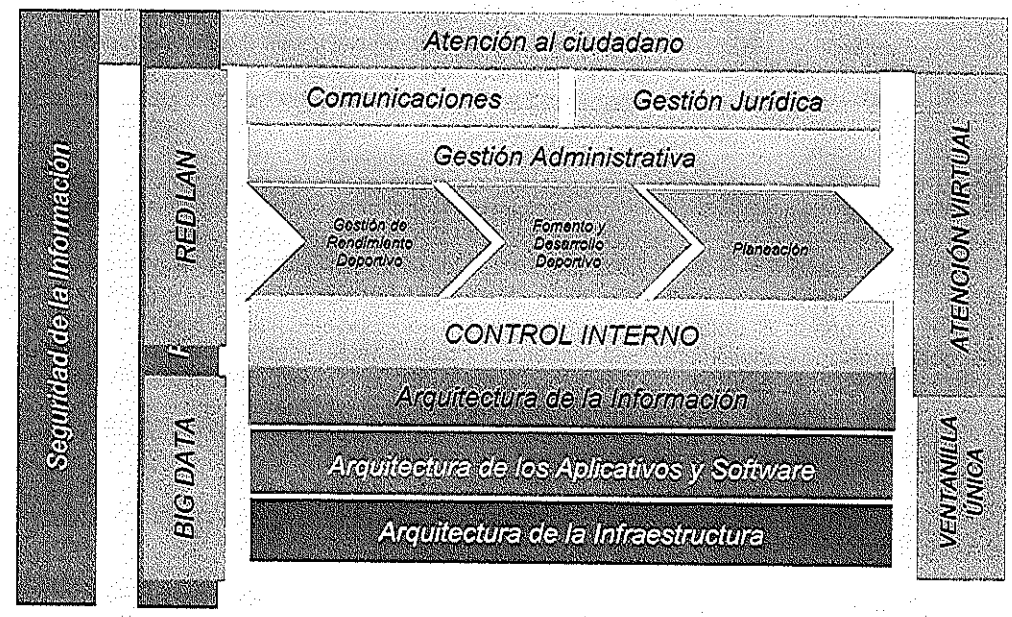


Imagen 3 Arquitectura empresarial alineada a los procesos de la entidad.

Arquitectura empresarial basada en TOGAF la cual se recomienda para implementar en la entidad la cual es el elemento principal de la Estrategia TI.

Arquitectura Empresarial TOGAF proporciona los métodos y herramientas para ayudar a la aceptación, la producción, el uso y el mantenimiento de una arquitectura empresarial, se basa en un modelo de proceso iterativo con el apoyo de las mejores prácticas y una re-utilizable con el conjunto de activos arquitectura existente, aprovechando los mapeos de TOGAF, con otras arquitecturas como los marcos de referencia de arquitectura de procesos(eTOM), Marco de referencia para datos e información (SID), Marco de referencia de tecnología(TAM).

La arquitectura empresarial incorpora el gobierno de TI a través de acuerdos de desarrollo de servicios y de implementación de facilidades tecnológicas. De esta manera los procesos de la entidad se adelantarán con énfasis en la eficiencia, la transparencia y el control de la gestión.

Para el desarrollo de la estrategia de TI se tendrán en cuenta las normas vigentes: como las disposiciones legales y la normatividad vigente expedida por las autoridades de naturaleza internas y externas.

La oficina de Tecnología y sistemas de información o quien haga sus veces expedirá políticas de alcance institucional, cómo las políticas de seguridad, acceso y uso de la información y de los recursos tecnológicos, las políticas de TI definidas desde la estrategia serán emitidas y publicadas mediante los mecanismos y procesos normativos que disponga la entidad.

9.1 Estrategia de Tecnología de la Información - TI

A continuación, siguiendo con el modelo de estrategia de TI, se realiza un direccionamiento organizacional en el cual se gestiona la estrategia de TI con la estrategia institucional, la arquitectura empresarial o institucional se gestiona con los mecanismos de Gobierno de TI, a través de políticas, acuerdos de desarrollo de servicios y de implementación de facilidades tecnológicas para los procesos de la entidad.

Se adelantan con énfasis en la eficiencia, la transparencia y el control de la gestión y necesidades institucionales con las políticas operativas y de seguridad de la información, portafolio de proyectos y servicios, arquitectura de información y sistemas de información, plataforma tecnológica que posee la oficina de Tecnología y sistemas de información para determinar las estrategias a apuntar en sus 6 dominios del marco de referencia.

9.2. Definición de los objetivos estratégicos de la Tecnología de la Información - TI

a) Integrar los sistemas de información de las diferentes dependencias del INDERVALLE que permitan la toma de decisiones sostenibles y eficientes.

b) Incentivar la competitividad y la innovación de la ciudad a través del empoderamiento y la confianza de la ciudadanía en el uso de TIC.

c) Fortalecer la gestión de las tecnologías de la información y comunicaciones (TIC), que permita la adopción de los estándares y lineamientos de la arquitectura empresarial para un desarrollo incluyente, sostenido, participativo y transparente dentro del INDERVALLE.

d) Habilitar las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de INDERVALLE y la eficiencia y transparencia del Estado.

e) Implementar el sistema de gestión de servicio para gestionar de manera formalizada los requisitos de la entidad, las demandas de la institución convirtiéndolas en servicios de TI, de acuerdo con la estrategia y el presupuesto.

f) Generar e implementar soluciones tecnológicas que provean en forma oportuna, eficiente y transparente la información necesaria para el cumplimiento de los fines misionales del INDERVALLE.

g) Incrementar la calidad y cantidad de los servicios en línea ofrecidos a los ciudadanos.

Dominios del marco de referencia de	Actividades	Producto
1. Estrategia de TI	Implementar la arquitectura empresarial, cumpliendo los lineamientos de la estrategia de Gobierno Digital de MINTIC	Procesos y procedimientos documentados.
2. Gobierno de TI	Implementar y documentar las políticas de seguridad de la información y política de tratamiento de riesgos al igual que la de gestión de infraestructura y tratamiento de información.	Cuadro de mando integral de gestión TIC – MSPI - MSDR
3. Gestión de información	Estrategias de Análisis de información Big Data y la publicación de catálogos de datos en la página de datos	Cumplimiento de las políticas del Modelo Integrado de Gestión MIPG -
4.Sistema de Información	Sistema de información para la ventanilla única	Implementación de la estrategia de atención al ciudadano, cumplimiento de la ley anti tramites, y seguridad y privacidad de los datos. Aplicativos que le permitan la toma eficiente de decisiones
5.Gestión de Servicios Tecnológicos	Plataforma de seguimiento de PQRSD, les permita a los usuarios ver el estado de las solicitudes en línea. Aplicativo de seguimiento a las	Aplicación de seguimiento y control de las solicitudes
6. Uso y apropiación de TIC	Capacitar y brindar a los usuarios de la entidad las opciones de seguimiento y a los ciudadanos les permita un acercamiento digital hacia la	Medir la satisfacción de los usuarios de los servicios prestados.

10. MODELO DE PLANEACIÓN

En esta fase se construye el plan estratégico de TI en el cual, se establece el modelo de operación; las estrategias por cada uno de los componentes del modelo; el modelo de planeación con la definición del portafolio de proyectos y la proyección de los recursos financieros.

10.1 Lineamientos y/o principios que rigen el Plan Estratégico de TIC

La definición y ejecución del PETI en INDERVALLE tiene como referente permanente los lineamientos establecidos por el MINTIC a través del Marco de Referencia de Arquitectura Empresarial en cada uno

de sus 6 dominios. Así mismo, se observan plenamente los lineamientos establecidos por la Estrategia de Gobierno en línea.

Adicionalmente, se observarán permanentemente como principios en la formulación e implementación del PETI:

a) La tecnología no es un fin en sí misma en tanto se pone al servicio del cumplimiento de las metas estratégicas y de gestión de la organización.
b) El compromiso y apropiación de la gestión de tecnologías de la información por parte de la alta dirección permitirá optimizar el uso de los recursos destinados a tecnología.
c) El PETI se considerará un instrumento dinámico que estará en permanente condición de actualización con objeto de maximizar su generación de valor para la entidad y se implementará a partir de los recursos disponibles en el INDERVALLE para tal fin y en todo caso se buscarán permanentemente fuentes de transferencia tecnológica y cooperación técnica y financiera que puedan apoyar su ejecución.

11. PROYECCIÓN DE PRESUPUESTO DEL ÁREA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN, TI

La proyección presupuestal se basa en cada una de las fases planteadas en el **PROYECTO DE MEJORA DE LA INFRAESTRUCTURA TECNOLÓGICA**, planteado en cada una de las fases:

Ítem	FASES	VALOR	TIEMPO DE EJECUCIÓN
1	Infraestructura Física	$ 250.000.000	4 a 8 semanas
2	Infraestructura Lógica	$ 100.000.000	4 a 8 semanas
3	Sistema de procesamiento y almacenamiento	$ 200.000.000	2 a 4 semanas
4	Sistema de protección eléctrica y almacenamiento	$ 500.000.000	18 a 24 semanas

12. PLAN DE COMUNICACIONES

Para generar condiciones óptimas de implementación, apropiación, uso y mejoramiento continuo en el marco del PETI, son necesarias acciones de divulgación y promoción de los alcances, actividades de formación, entrever los avances y documentación de transformaciones atribuibles a la estrategia de TI en el INDERVALLE.

Para este propósito, es necesario ordenar los canales de comunicación en torno a reportes de avance, contenidos informativos y a campañas pedagógicas de alcance básico. De forma incremental, la capacidad de la entidad para involucrar a los miembros de la entidad en las acciones de divulgación y promoción crecerá, para lo cual se tendrán en cuenta los siguientes canales y tipos de contenidos:

Canal	Metodología	Público Objetivo	Impacto Esperado	Oportunidad
Presencial	Presentaciones ejecutivas del PETI (apoyada en presentaciones de diapositivas, y/o videos, y preparadas con guiones)	- Gerencia - Subgerencias - Grupos de interesados de cada proyecto del PETI - Contratistas - Órganos de control y auditoría - Todo el personal interno	- Aprobación de alcance y portafolio de proyectos - Socialización de alcance de actividades - Reconocimiento de responsabilidades y sinergias - Revisión periódica de logros - Motivación interna y promoción de incentivos	- Anual - Al inicio de cada proyecto del PETI - Por requerimiento - Rendición de cuentas
Canales electrónicos	Taller de apropiación de propósito, metas, responsabilidades y sinergias en el marco del PETI	- Gerencia - Subgerencias - Dependencia de TI y Planeación - Contratistas - Todo el personal interno	- Alineación operativa, logística y conceptual para la implementación del PETI	- Semestral (Gerencia, Subgerencia de Planeación) - Anual (Todo el Personal)
	Boletín informativo de los avances y retos en la implementación del PETI vigente (a través de correo	- Todo INDERVALLE	- Alineación operativa, logística y conceptual para la implementación del PETI	- Trimestral - Rendición de Cuentas

13. ANEXOS

EQUIPOS PLATAFORMA TECNOLOGICA

DEPENDENCIA	EQUIPOS PCs	IMPRESORAS		ESCANER	
ALMACEN	4	HP Laser Jet P1606dn	1		
COMPETICION - CMD	12 – 9	HP Laser Jet P1102w HP Laser Jet M1132	2 1		

COMUNICACIONES	2	HP Laser Jet P1606dn	2		
CONTABILIDAD	4				
CONTROL INTERNO	6	HP Laser Jet P1606dn	1		
GERENCIA	3		1		
PRESUPUESTO	7				
RECAUDOS	1	HP Laser Jet P1606dn	1		
RECURSOS HUMANOS	5	HP Laser Jet P1606dn HP Laser Jet P1102w HP Laser Jet P1006 Epson LX300 II	1 1 1 1		
SECGRAL – ARCHIVO	8 – 2	HP Laser Jet P1606dn HP Laser Jet P1102w	1 1	Epson DS 530 Epson ES 400 Epson DS 510	1 1 1
SISTEMAS	2	Epson XP-211	1	Epson ES 400	1
SUBGERENCIA ADMINISTRATIVA CAD RENDICIONES	8 – 2 - 1	HP Laser Jet P1606dn HP Laser Jet P1102w Brother Label QL800	2 2 1	Epson DS 530 HP Pro 2500 FT	5 1
FOMENTO	5				
PLANEACION	9	HP Laser Jet P1606dn	1	Epson DS 530	1
TESORERIA	7	HP Laser Jet P1606dn HP Laser Jet P1102w	1 1		
Total	**97**		**23**		**11**

DEPENDENCIA	PORTATILES
Almacén	1
CMD	4
Comunicaciones	1
Gerencia	2
Subgerencia Administrativa	2
Subgerencia de Competición	4
Subgerencia de Fomento	1
Subgerencia de Planeación	1
Total	**16**

Elaboró:	Revisó:	Aprobó	Incorporó SGI
Nombre: Stella Jiménez Pimentel	Nombre: Rafael Pérez Manquillo	Nombre: Carlos Felipe López López	Nombre: Rodrigo Martínez Cruz
Cargo: Técnico Operativo	Cargo: Subgerente Administrativo y Financiero	Cargo: Gerente	Cargo: Jefe Oficina Asesora de Planeación
Firma:	**Firma:**	**Firma:**	**Firma:**