



Alcaldía  
de Yumbo



**IMDERTY**  
INSTITUTO MUNICIPAL DEL DEPORTE  
Y LA RECREACIÓN DE YUMBO

# INSTITUTO MUNICIPAL DEL DEPORTE Y LA RECREACIÓN DE YUMBO - IMDERTY

## PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**YOAN URIEL SUÁREZ QUINTERO**  
**GERENTE IMDERTY**

**ENERO – 2024**



Alcaldía  
de Yumbo

Dirección IMDERTY: Carrera 4 No. 16-199 – Yumbo, Valle del Cauca  
Teléfonos: 602 6697822 - 602 6697844 - 602 6697828  
E-mail: [ventanilla@imderty.gov.co](mailto:ventanilla@imderty.gov.co)



[www.imderty.gov.co](http://www.imderty.gov.co)



[Imderty Yumbo](#)



[Imderty Yumbo](#)



[imderty\\_yumbo](#)



**IMDERTY**  
INSTITUTO MUNICIPAL DEL DEPORTE  
Y LA RECREACIÓN DE YUMBO



Alcaldía  
de Yumbo



IMDERTY  
INSTITUTO MUNICIPAL DEL DEPORTE  
Y LA RECREACIÓN DE YUMBO

## TABLA DE CONTENIDO

	PÁG.
1. INTRODUCCIÓN.....	3
2. OBJETIVO.....	3
OBJETIVO GENERAL .....	3
OBJETIVOS ESPECÍFICOS .....	3
3. DIRECCIONAMIENTO ESTRATÉGICO.....	4
ALCANCE.....	¡Error! Marcador no definido.
MISIÓN.....	¡Error! Marcador no definido.
VISIÓN .....	¡Error! Marcador no definido.
PRINCIPIOS ÉTICOS.....	¡Error! Marcador no definido.
VALORES EMPRESARIALES.....	¡Error! Marcador no definido.
OBJETIVOS ESTRATÉGICOS .....	¡Error! Marcador no definido.
4. MARCO NORMATIVO.....	5
5. CONCEPTOS ASOCIADOS.....	8
6. COMPONENTES DEL PLAN .....	9
IMPORTANCIA DE LA SEGURIDAD DE INFORMACIÓN .....	9
MARCO DE TRABAJO DE PROYECTOS .....	9
PROYECTOS ESTRATÉGICOS .....	10
PROGRAMACIÓN 2024.....	11
ACTUALIZACIÓN DEL PESI .....	11
7. REFERENCIAS .....	12
8. CONTROL DE CAMBIOS .....	¡Error! Marcador no definido.
9. APROBACIÓN .....	¡Error! Marcador no definido.



Alcaldía  
de Yumbo

Dirección IMDERTY: Carrera 4 No. 16-199 – Yumbo, Valle del Cauca

Teléfonos: 602 6697822 - 602 6697844 - 602 6697828

E-mail: [ventanilla@imderty.gov.co](mailto:ventanilla@imderty.gov.co)



[www.imderty.gov.co](http://www.imderty.gov.co)



Imderty Yumbo



Imderty Yumbo



imderty\_yumbo



IMDERTY  
INSTITUTO MUNICIPAL DEL DEPORTE  
Y LA RECREACIÓN DE YUMBO



Alcaldía  
de Yumbo



IMBERTY  
INSTITUTO MUNICIPAL DEL DEPORTE  
Y LA RECREACIÓN DE YUMBO

## 1. INTRODUCCIÓN

El progreso y éxito de países, instituciones y empresas dependen esencialmente del uso efectivo de las tecnologías de la información y la comunicación. En este contexto, la información manejada se convierte en un activo cada vez más valioso, capaz de influir directamente en el éxito u fracaso de una organización. Por lo tanto, resulta crucial implementar herramientas y procesos que aseguren, respalden y mantengan la información de manera óptima y redundante.

A pesar de la importancia vital de la seguridad informática, muchas empresas subestiman los riesgos actuales, incluyendo amenazas internas como errores humanos y amenazas externas como virus. La falta de inversión en capital humano y recursos económicos para prevenir daños o pérdidas de información conlleva a datos poco confiables, integridad comprometida y falta de disponibilidad, lo que puede resultar en la paralización de operaciones y pérdidas significativas de tiempo y dinero, elementos cruciales para el desarrollo de cualquier organización.

En respuesta a estos desafíos, las instituciones desarrollan el Plan Estratégico de Seguridad y Privacidad de la Información (PESI). Este plan tiene como objetivo reducir o abordar las vulnerabilidades y riesgos asociados con la seguridad de la información, convirtiéndose en una parte esencial de las actividades estratégicas de las organizaciones. Su implementación garantiza un entorno seguro y confiable para el manejo de la información, respaldando así el crecimiento y desarrollo sostenible de la empresa.

## 2. OBJETIVO

### Objetivo general

Implementar el Plan Estratégico de Seguridad y Privacidad de la Información a través de proyectos que permitan establecer, implementar, operar, monitorear, revisar y una mejora continua de la institución.

### Objetivos específicos

- Salvaguardar la integridad de la información a través de las buenas prácticas de seguridad y privacidad de la información.
- Definir proyectos a realizar dentro del alcance del plan, teniendo en cuenta, alcance, tiempo y presupuesto.
- Asociar los objetivos de cada proyecto a dar solución a los riesgos expuestos en la matriz de riesgos de seguridad informática de la empresa.
- Desarrollar los proyectos dentro los tiempos y lineamientos establecidos por la empresa.



Alcaldía  
de Yumbo

Dirección IMBERTY: Carrera 4 No. 16-199 – Yumbo, Valle del Cauca  
Teléfonos: 602 6697822 - 602 6697844 - 602 6697828  
E-mail: [ventanilla@imderty.gov.co](mailto:ventanilla@imderty.gov.co)



[www.imderty.gov.co](http://www.imderty.gov.co)



Imderty Yumbo



Imderty Yumbo



imderty\_yumbo



IMBERTY  
INSTITUTO MUNICIPAL DEL DEPORTE  
Y LA RECREACIÓN DE YUMBO

### 3. DIRECCIONAMIENTO ESTRATÉGICO

**Misión de TI:** Utilizar las Tecnologías de la Información y Comunicaciones de manera innovadora y efectiva para optimizar la gestión, promoción y acceso a las actividades deportivas y recreativas. Nuestra misión es aprovechar las TIC para facilitar la participación ciudadana, mejorar la eficiencia operativa y enriquecer la experiencia deportiva, contribuyendo al bienestar y desarrollo integral de la comunidad.

**Visión de TI:** Convertirnos en un referente a nivel local en la integración de Tecnologías de la Información y Comunicaciones para el fomento del deporte y la recreación. Buscamos liderar la innovación digital en el ámbito deportivo, proporcionando plataformas tecnológicas avanzadas que promuevan la participación de la comunidad, la eficiencia en la gestión y la creación de experiencias enriquecedoras para todos los usuarios, contribuyendo así al desarrollo integral y saludable de la sociedad.

#### Alcance

El Plan Estratégico de Tecnologías de Información y Comunicaciones (PETIC), busca generar estrategias que lleven a la correcta implementación de proyectos de TI de acuerdo con el marco de referencia de MinTIC, el cual hace parte de la planeación estratégica del Instituto y pretende desarrollar los siguientes puntos:

- Un portafolio de Proyectos de TI.
- Modelo de Gestión de TIC.
- Modelo de Gobierno de TIC.
- Definición de los diferentes Planes transversales al PETIC como el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Plan Estratégico de Tratamiento Riesgos de Seguridad y Privacidad de la Información.

#### 2.1. Misión

Promover la práctica de la educación física, el deporte, la recreación y el aprovechamiento del tiempo libre, contribuyendo al desarrollo humano integral y el mejoramiento de la calidad de vida de los habitantes del municipio de Yumbo.

## 2.2. Visión

Posicionar al municipio de Yumbo como modelo deportivo departamental y nacional reconocido por sus valores humanos y los logros en educación física, deporte, recreación y aprovechamiento del tiempo libre.

## 4. MARCO NORMATIVO

El presente Plan Estratégico en Tecnologías de Información y Comunicaciones (PETIC) está regido por las siguientes Leyes, decretos y lineamientos de orden nacional y territorial que sirven como parámetro y guía para el desarrollo adecuado del plan:

- **Decreto 612 de 2018:** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.
- **Decreto 415 de 2016 Artículo 2.2.35.3:** Objetivos del fortalecimiento institucional.
- **Decreto 1078 de 2015 Artículo 2.2.5.1.2.2:** Instrumentos - Marco de Referencia de Arquitectura Empresarial para la gestión de TI.
- **Ley 1712 de 2014:** Ley de transparencia y de acceso a la información pública nacional.
- **Decreto Nacional 2573 de 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- **Directiva Presidencial No. 04 de 2012:** Eficiencia Administrativa y Lineamientos de la Política de Cero Papel en la Administración Pública.
- **Decreto 019 de 2012:** Ley anti-trámites.
- **Decreto 2693 de 2012:** Lineamientos generales de la estrategia de gobierno en línea para la Nación.
- **Ley 1474 de 2011:** Ley anticorrupción.
- **Ley 1273 de 2009:** De la protección de la información y los datos.

- **Decreto 1151 de 2008:** Mediante el cual se establecen los lineamientos generales de la Estrategia de Gobierno En Línea, que son de obligatorio cumplimiento para las entidades que conforman la administración pública en Colombia.
- **Ley 962 de 2005:** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos Administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2482 de 2012:** Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión.
- **Decreto Ley 019 de 2012:** Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Ley 1437 de 2011:** Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 1341 de 2009:** Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley 527 de 1999:** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Documento CONPES 3920 de 2018:** Política Nacional de Explotación de Datos (Big Data)
- **Decreto 1413 de 2017:** Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- **Decreto 849 de 2016:** Por el cual se modifica la estructura del Departamento Administrativo de Ciencia, Tecnología e Innovación – COLCIENCIAS.
- **Documento CONPES 3854 de 2016:** Política Nacional de Seguridad Digital.
- **Decreto 415 de 2016:** Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- **Ley 1753 de 2015:** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”.
- **Decreto 1083 de 2015:** Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014 que establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital).
- **Decreto 1078 de 2015:** Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea.
- **Decreto 103 de 2015:** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 en lo relativo a la gestión de la información pública y se dictan otras disposiciones.
- **Ley 1712 de 2014:** Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

## 5. CONCEPTOS ASOCIADOS

Para el desarrollo del presente Plan, es importante tener en cuenta las definiciones que a continuación se establecen en concordancia con lo estipulado por el Departamento Administrativo de la Función Pública -DAFP.

**Factores de riesgos:** Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser interna o externa a la entidad.

**Impacto:** Es la medición y valoración del daño que podría producir a la empresa un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.

**Riesgo:** Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

**Seguridad:** Cualidad o estado de seguro. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

**Seguridad física:** Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir procesamiento de información.

**Seguridad lógica:** Consiste en la aplicación de barreras y procedimientos para mantener la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

**Seguridad de las redes:** Es la capacidad de las redes para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes ofrecen o hacen accesibles y que son tan costosos como los ataques intencionados.

**Seguridad Informática:** Son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

**Vulnerabilidad:** Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.

## 6. COMPONENTES DEL PLAN

### Importancia de la Seguridad de Información

La información se considera la materia prima más valiosa para instituciones, empresas y corporaciones, siendo esencial para el funcionamiento de la planeación estratégica. En el caso de empresas automatizadas, su seguridad sigue siendo un punto crítico y determinante para evitar fracasos.

A pesar de que consideremos nuestra institución como segura, el creciente uso de nuevas tecnologías para gestionar información nos expone a un mayor número y variedad de amenazas. En el entorno competitivo actual, es vital que las entidades garanticen la confidencialidad, integridad y disponibilidad de su información corporativa clave.

La seguridad informática debe surgir de la colaboración entre los responsables de seguridad de la información y los usuarios, quienes deben ser conscientes de los riesgos asociados con ciertos usos de los sistemas y recursos. Problemas de seguridad implican pérdida de tiempo y recursos durante la recuperación de la actividad normal, que en muchos casos es irreparable.

La responsabilidad de la concienciación recae en los responsables de seguridad de la información, respaldados de manera activa por la Dirección. Es crucial informar sobre las principales amenazas y las acciones a tomar para evitarlas, estableciendo procedimientos efectivos que complementen las medidas técnicas implementadas por el equipo de informática.

En este nuevo entorno, las empresas deben prepararse no solo para prevenir riesgos que comprometan operaciones comerciales, sino también para establecer medidas que reduzcan problemas potenciales de seguridad.

El objetivo de este documento es presentar un marco de trabajo para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la información del IMDERTY. Con esta iniciativa, se busca fortalecer la seguridad y privacidad de los datos, proteger los recursos y garantizar la confianza de clientes y socios en el manejo de la información.

### Marco de Trabajo de Proyectos

El programa estratégico de seguridad de la información se desarrolla siguiendo los lineamientos dados por los siguientes documentos:

- ISO 27001
- Autoevaluación MSPI

- Análisis de vulnerabilidades y riesgos de TI de la empresa.
- Programa de tratamiento de Riesgos
- Artículo 6 - Ley 1581 de 2012: Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles.
- Artículo 17 - Ley 1581 de 2012: Deberes de los responsables del Tratamiento. Los responsables del Tratamiento deberán cumplir los deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad.
- Artículo 18 - Ley 1581 de 2012: Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad.
- Artículo 13 - Ley 1712 de 2014: Registros de Activos de Información. Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información.
- Artículo 17 - Ley 1712 de 2014: Sistemas de información. Para asegurar que los sistemas de información electrónica sean efectivamente una herramienta para promover el acceso a la información pública

Con la información recolectada por los documentos anteriores se define según la prioridad y las buenas prácticas de seguridad informática, los proyectos alienados a dar cumplimiento a las políticas y estándares nacionales en materia de TI. Se define un plazo de ejecución para la vigencia 2024, teniendo en cuenta el alcance, tiempo, riesgo y presupuesto.

## Proyectos Estratégicos

**Tabla 1: Proyectos Estratégicos**

1	Definir e implementar un Plan Estratégico de Seguridad y Privacidad de la Información.
2	Definir e implementar un Plan Estratégico de Tratamiento de Riesgos y de Seguridad y Privacidad de la Información.
3	Estandarizar los equipos y sistemas.
4	Definir los Activos de Información.
5	Definir los Procesos y Procedimiento del área de TI.
6	Definir un Portafolio de Planes y Proyectos de TI.
7	Implementar un servicio de automatización de backups.
8	Definir e implementar la Política de Gobierno Digital.
9	Definir e implementar la Política de Seguridad Digital.
10	Definir e implementar la Política de Transparencia y Acceso a la Información.
11	Definir el Portafolio de servicios.
12	Definir un Plan de Continuidad de TI.
13	Sistematizar los sistemas de información.
14	Implementar un servicio de gestión documental

## Programación 2024



A continuación, se muestra una propuesta de programación para la ejecución de los proyectos y actividades del PESI, el tiempo de ejecución de las actividades es de 1 año:

**Tabla 2: Programación 2024**

PROGRAMACIÓN	
1	Definir e implementar un Plan Estratégico de Seguridad y Privacidad de la Información.
2	Definir e implementar un Plan Estratégico de Tratamiento de Riesgos y de Seguridad y Privacidad de la Información.
3	Estandarizar los equipos y sistemas.
4	Definir los Activos de Información.
5	Definir los Procesos y Procedimiento del área de TI.
7	Implementar un servicio de automatización de backups.
14	Implementar un servicio de gestión documental

**Tabla 3: Programación 2024**

ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC

### Actualización del PESI

Este programa estratégico se podrá actualizar dependiendo de los cambios en la estratégica organizacional de la institución, cambios o daños significativos en la infraestructura tecnológica de la empresa, incidentes de seguridad o privacidad de la información que tengan un impacto general muy alto, hay que tener en cuenta que las modificaciones de este programa solo podrán ser autorizadas con el visto bueno de la dirección, el personal de informática y el personal de planeación estratégica de la institución.



Dirección IMDERTY: Carrera 4 No. 16-199 – Yumbo, Valle del Cauca  
Teléfonos: 602 6697822 - 602 6697844 - 602 6697828  
E-mail: [ventanilla@imderty.gov.co](mailto:ventanilla@imderty.gov.co)



[www.imderty.gov.co](http://www.imderty.gov.co)



imderty Yumbo



imderty Yumbo



imderty\_yumbo



## 7. REFERENCIAS

M. Hernández, "Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial" (Tesis, Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral, 2006).

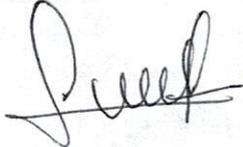
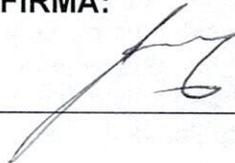
Echenique García José Antonio, Auditoria en Informática (2da Edición, Mc. Graw Hill, 2001), pp. 194-241.

Laudon Kenneth C. y Laudon Jane P, Administración de los Sistemas de Información, Organización y Tecnología (3ra Edición, México, Prentice Hall Hispanoamericana S.A., 1994), pp. 702-706.

Lucena López Manuel José, Criptografía y Seguridad en Computadoras (2da Edición, Universidad de Jaen, 1999), pp. 30-138.

Norton Peter, Introducción a la Computación (1ra Edición, México, Mc Graw Hill), pp. 50-53.  
Simson Garfinkel y Spafford Gene, Seguridad y Comercio en el Web (México, Mc. Graw Hill, 1999), pp. 8-13.

Simson Gar Finkel, y Spafford Gene, Seguridad Práctica en UNIX e Internet (2da Edición, Mc. Graw Hill, 1999), pp.360-366.

<p><b>ELABORO Y REVISÓ:</b> SANDRA V. TOBAR GARCÍA</p>	<p><b>CARGO:</b> SUBGERENTE ADMINISTRATIVA Y FINANCIERA</p>	<p><b>FIRMA:</b> </p>
<p><b>APROBÓ:</b> YOAN U. SUÁREZ QUINTERO</p>	<p><b>CARGO:</b> GERENTE</p>	<p><b>FIRMA:</b> </p>