


 <b>Indeportes</b>   CAUCA	<b>POLÍTICA DE SEGURIDAD DIGITAL</b>		 <b>Gobernación del Cauca</b>
	<b>SISTEMAS DE INFORMACION Y COMUNICACIÓN</b>		
<b>FECHA:</b> 2024/05/10	<b>CÓDIGO:</b> A-TIC- PP- 002	<b>VERSIÓN:</b> 01	<b>PÁGINA:</b> 1 de 7



## POLÍTICA SEGURIDAD DIGITAL

**MAYO  
2024**

	POLÍTICA DE SEGURIDAD DIGITAL		 <b>Gobernación del Cauca</b>
	SISTEMAS DE INFORMACION Y COMUNICACIÓN		
FECHA: 2024/05/10	CÓDIGO: A-TIC- PP- 002	VERSIÓN: 01	PÁGINA: 2 de 7

## CONTENIDO

1. INTRODUCCIÓN.....	3
2. OBJETIVOS.....	3
3. NORMATIVIDAD .....	4
4. ALCANCE.....	4
5. RESPONSABILIDADES .....	4
6. TÉRMINOS Y DEFINICIONES.....	4
7. DESARROLLO .....	4
8. SEGUIMIENTO Y EVALUACIÓN.....	5
9. ANEXOS.....	6
10. CONTROL DE CAMBIOS .....	6

	<b>POLÍTICA DE SEGURIDAD DIGITAL</b>		 <b>Gobernación del Cauca</b>
	<b>SISTEMAS DE INFORMACION Y COMUNICACIÓN</b>		
<b>FECHA:</b> 2024/05/10	<b>CÓDIGO:</b> A-TIC- PP- 002	<b>VERSIÓN:</b> 01	<b>PÁGINA:</b> 3 de 7

## 1. INTRODUCCIÓN

Debido al incremento a nivel tecnológico que se vive en la actualidad en cuanto a la digitalización de la información y los procesos de la era digital, se ha evidenciado un aumento importante en las amenazas y riesgos cibernéticos, los cuales pueden tener un impacto negativo en la entidad, teniendo como resultado pérdida de información sensible, pérdida de imagen reputacional o no conformidades por parte de los entes de control, por lo anterior con la finalidad de dar cumplimiento a las normas y regulaciones se crea la Política de Seguridad Digital.

De acuerdo al Modelo Integrado de Planeación y Gestión (MIPG) el cual establece las directrices para fortalecer la gestión pública, en este caso la Seguridad Digital, busca proteger la información y los sistemas de información, implementando medidas de seguridad informática, gestión de riesgo, protección de datos y la ciberseguridad general, con este fin se desea encaminar esta Política de Seguridad Digital permitiendo contrarrestar cualquier amenaza, manteniendo la confianza de las partes interesadas, mejorando la eficiencia y la productividad de la entidad.

En el presente documento se encuentra la Política de Seguridad Digital para INDEPORTES CAUCA, adoptando los lineamientos dados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) bajo el modelo de MIPG, esta política busca promover la Disponibilidad, Integridad, Confidencialidad y Autenticidad de la información, lo cual es crucial en el entorno de la gestión pública, ya que está basada en la protección de la información sensible de los usuarios y en la garantía de la continuidad de los diferentes servicios digitales.



## 2. OBJETIVOS

### ➤ GENERAL

Elaborar y definir la Política de Seguridad Digital con sus respectivos lineamientos con la finalidad de identificar, gestionar, tratar y mitigar los riesgos de seguridad digital de INDEPORTES CAUCA en su entorno digital, garantizando la protección de la información, sistemas y las redes digitales contra posibles amenazas.

### ➤ ESPECIFICO

- Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en INDEPORTES CAUCA.
- Promover en el personal de INDEPORTES CAUCA las buenas prácticas en el uso del entorno digital.
- Controlar el acceso y descarga de software no autorizado en los equipos de INDEPORTES CAUCA.
- Proteger los activos de la información de INDEPORTES CAUCA.

 <b>Indeportes</b>   CAUCA	<b>POLÍTICA DE SEGURIDAD DIGITAL</b>		 <b>Gobernación del Cauca</b>
	<b>SISTEMAS DE INFORMACION Y COMUNICACIÓN</b>		
<b>FECHA:</b> 2024/05/10	<b>CÓDIGO:</b> A-TIC- PP- 002	<b>VERSIÓN:</b> 01	<b>PÁGINA:</b> 4 de 7

### 3. NORMATIVIDAD

- Decreto 1599 de 2005, mediante el cual se crea el Modelo Estándar de Control Interno.
- Decreto 1499 de 2017 modelo integrado de planeación y gestión.
- Decreto 612 de 2018 plan de acción.
- Ley 1474 de 2011 estatuto anticorrupción.
- Ley 1712 de 2014 ley de transparencia.
- NTC ISO/IEC 27001: 2022.
- Decreto 2693 de 2012: lineamientos generales de la estrategia de gobierno en línea de la república de Colombia que lidera el ministerio de las tecnologías de información y las comunicaciones.

### 4. ALCANCE

Se establece que la Política de Seguridad Digital tiene como alcance la protección de los activos de información de los cuales hacen uso todos los funcionarios en INDEPORTES CAUCA, esto con el objetivo de minimizar los riesgos de la información.



### 5. RESPONSABILIDADES

### 6. TÉRMINOS Y DEFINICIONES

- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MINTIC:** Ministerio Tecnologías de la Información y la Comunicación.
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital.
- **TIC:** Las Tecnologías de la Información y las Comunicaciones.
- **Confidencialidad:** Se refiere a que la información solo puede ser conocida por individuos autorizados.
- **Integridad:** Los datos están protegidos de cambios no autorizados para garantizar que son fiables y correctos.
- **Disponibilidad:** Principio el cual asegura la fiabilidad y el acceso oportuno de la información por parte de los usuarios.
- **Autenticidad:** Asegura que la organización dispone de información legítima, garantizando el autor de la información o documento.

### 7. DESARROLLO

La Política de Gobierno Digital contiene los lineamientos, objetivos y estrategias establecidas para el uso y correcto aprovechamiento de las tecnologías de la información y las comunicaciones, según el marco integrado de planeación y gestión, con la finalidad de dar cumplimiento a la norma INDERPORTES CAUCA, comprometida con el desarrollo de la entidad, adopta esta política fortaleciendo el proceso de gestión pública, transparencia de la información y eficiencia de los respectivos procesos, asegurando el cumplimiento los pilares de la seguridad de la información.

	<b>POLÍTICA DE SEGURIDAD DIGITAL</b>		 <b>Gobernación del Cauca</b>
	<b>SISTEMAS DE INFORMACION Y COMUNICACIÓN</b>		
<b>FECHA:</b> 2024/05/10	<b>CÓDIGO:</b> A-TIC- PP- 002	<b>VERSIÓN:</b> 01	<b>PÁGINA:</b> 5 de 7

## 8. SEGUIMIENTO Y EVALUACIÓN

Para el seguimiento de la Política de Seguridad Digital se tendrá como objetivo principal la protección de la información, con el fin de minimizar el impacto de los riesgos identificados para los activos de la información de INDEPORTES CAUCA, permitiendo responder a los 3 pilares de la Seguridad de la Información.

PROPOSITO	OBJETIVO
Uso de Correo Electrónico	<ul style="list-style-type: none"> <li>• La cuenta de correo electrónico institucional es personal e intransferible, por seguridad la clave de todos los correos será cambiada cada 3 meses.</li> <li>• La cuenta de correo electrónico solo puede ser usada con funciones misionales del servidor público.</li> <li>• Los funcionarios públicos serán los responsables de depurar el buzón del correo periódicamente con el objetivo de evitar que se sature de información no necesaria.</li> <li>• Una vez un servidor público se le asigna correo institucional y este sale de la misma, debe realizar entrega de las credenciales y la información de importancia para la entidad.</li> </ul>
Equipos Institucionales	<ul style="list-style-type: none"> <li>• Los equipos de cómputo, Tablet, Dispositivos de almacenamiento, no deben salir de la institución sin previa aprobación del jefe de área encargado.</li> <li>• El equipo de cómputo asignado es de uso</li> </ul>

 <b>Indeportes CAUCA</b>	<b>POLÍTICA DE SEGURIDAD DIGITAL</b>		 <b>Gobernación del Cauca</b>
	<b>SISTEMAS DE INFORMACION Y COMUNICACIÓN</b>		
<b>FECHA: 2024/05/10</b>	<b>CÓDIGO: A-TIC- PP- 002</b>	<b>VERSIÓN: 01</b>	<b>PÁGINA: 6 de 7</b>
		<p>único para la ejecución de funciones asignadas por INDEPORTES CAUCA.</p> <ul style="list-style-type: none"> <li>• Los funcionarios no pueden realizar ningún tipo de descarga de software, música o archivos de fuentes no confiables debido a que debe estar totalmente licenciado.</li> </ul>	
	Contraseñas	<ul style="list-style-type: none"> <li>• Las contraseñas de los equipos de cómputo serán asignadas por el área encargada, dando cumplimiento a criterios tales como:</li> <li>• Al menos 8 caracteres.</li> <li>• Combinación de mayúsculas, minúsculas, números y caracteres especiales.</li> <li>• Evitar palabras comunes o secuencias obvias.</li> </ul>	
	Acceso a la Red	<ul style="list-style-type: none"> <li>• El área encargada realizara el bloqueo de páginas web las cuales representen riesgo potencial para la entidad tales como:</li> <li>• Redes sociales.</li> <li>• Contenido adulto.</li> <li>• Hacking.</li> <li>• Descargas.</li> <li>• Apuestas.</li> <li>• Plataformas de Entretenimiento.</li> </ul>	

## 9. ANEXOS

Este campo es opcional, en él se debe consignar la relación de documentos internos y externos a consultar como apoyo a un proceso.

## 10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
01	2024/05/10	Elaboración de la Política de Seguridad Digital

ELABORÓ		REVISÓ		APROBÓ	
Nicolas Alexander Diaz Martínez Contratista de TIC		Mónica Mera Cerón Jefe de Planeación Institucional		Acta N°3 Comité de Gestión y Desempeño Resolución 118 del 27 de junio 2024	
Fecha	2024/05/10	Fecha	2024/05/10	Fecha	2024/05/10