
 <b>INDERHUILA</b>	<b>DOCUMENTO APOYO</b>	<b>CODIGO</b>	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>VERSIÓN</b>	1
		<b>VIGENCIA</b>	ENERO 2021

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




**INDERHUILA**

**NEIVA, ENERO DE 2022**

 <b>INDERHUILA</b>	<b>DOCUMENTO APOYO</b>	<b>CODIGO</b>	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>VERSIÓN</b>	1
		<b>VIGENCIA</b>	ENERO 2021

## CONTENIDO

<b>INTRODUCCION .....</b>	<b>3</b>
<b>1. TERMINOS Y DEFINICIONES.....</b>	<b>3</b>
<b>2. OBJETIVO .....</b>	<b>6</b>
<b>2.1. OBJETIVOS ESPECIFICOS .....</b>	<b>6</b>
<b>3. RECURSOS .....</b>	<b>6</b>
<b>4. RESPONSABLES .....</b>	<b>7</b>
<b>5. METODOLOGÍA DE IMPLEMENTACIÓN.....</b>	<b>7</b>
<b>6. ACTIVIDADES PARA LA IMPLEMENTACION .....</b>	<b>8</b>
<b>7. CUMPLIMIENTO DE IMPLEMENTACIÓN .....</b>	<b>12</b>
<b>8. CRONOGRAMA .....</b>	<b>13</b>
<b>9. SEGUIMIENTO y EVALUACIÓN .....</b>	<b>14</b>
<b>10. ENTREGABLES .....</b>	<b>14</b>

 <b>INDERHUILA</b>	<b>DOCUMENTO APOYO</b>	<b>CODIGO</b>	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>VERSIÓN</b>	1
		<b>VIGENCIA</b>	ENERO 2021

## INTRODUCCION

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


### 1. TERMINOS Y DEFINICIONES

**Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

**Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

**Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

 <b>INDERHUILA</b>	<b>DOCUMENTO APOYO</b>	<b>CODIGO</b>	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>VERSIÓN</b>	1
		<b>VIGENCIA</b>	ENERO 2021

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

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


**Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

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

**Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

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

 INDERHUILA	DOCUMENTO APOYO		CODIGO	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>		VERSIÓN	1
			VIGENCIA	ENERO 2021

**Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.


**Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

**Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación

**Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

**Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

 <b>INDERHUILA</b>	<b>DOCUMENTO APOYO</b>	<b>CODIGO</b>	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>VERSIÓN</b>	1
		<b>VIGENCIA</b>	ENERO 2021

## 2. OBJETIVO

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

### 2.1. OBJETIVOS ESPECIFICOS

Implementar las Políticas de la seguridad de la información

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

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

## 3. RECURSOS

**Humano:** la Dirección, Líderes de los Procesos.

**Físico:** Servidores, Firewall, PC y equipos de comunicación

**Financiero:** Plan de Adquisiciones


## 4. RESPONSABLES

Dirección

Líderes de los Proceso

## 5. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en el Inderhuila, se toma referencia la metodología PHVA (Planear,

 <b>INDERHUILA</b>	<b>DOCUMENTO APOYO</b>		<b>CODIGO</b>	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>		<b>VERSIÓN</b>	1
			<b>VIGENCIA</b>	ENERO 2021

Hacer, Verificar y Actuar) y los lineamientos emitidos por el Manual de implementación versión 3.02 del Ministerio de Tecnologías de la Información y las Comunicaciones.

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

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




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

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

## 6. ACTIVIDADES PARA LA IMPLEMENTACION

1. Realizar Diagnóstico
2. Implementar políticas enfocadas a la seguridad de la Información.
3. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

 INDERHUILA	DOCUMENTO APOYO		CODIGO	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>		VERSIÓN	1
			VIGENCIA	ENERO 2021

4. Realizar Inventario de Activos de Información con los líderes de cada Proceso.

#### **Levantamiento del inventario de Activos en la institución**

5. Realizar la Valoración de los Activos de Información con los líderes de cada Proceso
6. Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)
7. Socializar el Plan de Tratamiento de Riesgo
8. Realizar seguimiento del Plan de Tratamiento de Riesgo

#### 7. CUMPLIMIENTO DE IMPLEMENTACIÓN

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

Implementar la Política de Seguridad de la información.

Implementar la Política de Administración de datos.

Implementar la Políticas de Comunicaciones.

Aspectos organizativos de la seguridad de la información

Seguridad de la Información enfocada a los recursos humanos

Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.


Revisión de los Controles de acceso

Seguridad Física y del entorno

Seguridad en las telecomunicaciones

Gestión de Incidentes de Seguridad de la Información



	DOCUMENTO APOYO		CODIGO	PA-GTIC-DA02
	<b>PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>		VERSIÓN	1
			VIGENCIA	ENERO 2021

Aspectos de seguridad de la información en la gestión de continuidad del negocio.

## 8. CRONOGRAMA

No.	ACTIVIDAD	RESPONSABLE	FECHA DE IMPLEMENTACION
1	Realizar Diagnóstico para levantar los activos de Información	Profesional Universitario TICS Lideres de Procesos	Junio 2022
2	Implementar la política enfocadas a la seguridad de la Información.	Profesional Universitario TICS Lideres de Procesos	Diciembre de 2022



**JORGE GARCIA QUIROGA**  
Director



Cruzval Alberto Rodriguez M.  
Elaborado por: