

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**- FONCOLOMBIA -
FONDO MIXTO PARA EL DESARROLLO
INTEGRAL Y LA GESTIÓN SOCIAL DE
COLOMBIA**

Tabla de contenido

INTRODUCCION.....	3
1. TÉRMINOS Y DEFINICIONES.....	3
2. OBJETIVO	5
2.1. OBJETIVOS ESPECIFICOS	5
3. RECURSOS.....	6
4. RESPONSABLES	6
5. METODOLOGÍA DE IMPLEMENTACIÓN	6
6. ACTIVIDADES PARA LA IMPLEMENTACION.....	7
7. CUMPLIMIENTO DE IMPLEMENTACIÓN.....	7
8. CRONOGRAMA	8
9. SEGUIMIENTO y EVALUACIÓN	9
10. ENTREGABLES	9

INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer cómo 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. TÉRMINOS 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).
- **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)
- **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).

2. OBJETIVO

Tratar y Monitorear los riesgos asociados a los procesos existentes de FONCOLOMBIA 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

- Elaborar un plan de trabajo para la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Aplicar las metodologías del DAFP o de la ISO respectivamente en seguridad y riesgo de la información.

Dirección: Carrera 51 #50-43 Barrio Los Cedros, Bucaramanga – Santander

Teléfono: (+57) 323 2299 720

Email: contacto@foncolombia.org.co

Horario: Lun a Vie 8:00 AM - 6:00 PM y Sab 8:00 AM - 12:00 M

3. RECURSOS

- **Humano:** Director ejecutivo, Jefes de oficina, trabajadores y/o contratista encargado de la oficina TIC.
- **Físico:** Equipos de cómputo, portátiles e impresoras.

4. RESPONSABLES

- Director ejecutivo
- Jefes de oficina
- Funcionario y/o contratista encargado de la oficina TIC.

5. METODOLOGÍA DE IMPLEMENTACIÓN

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

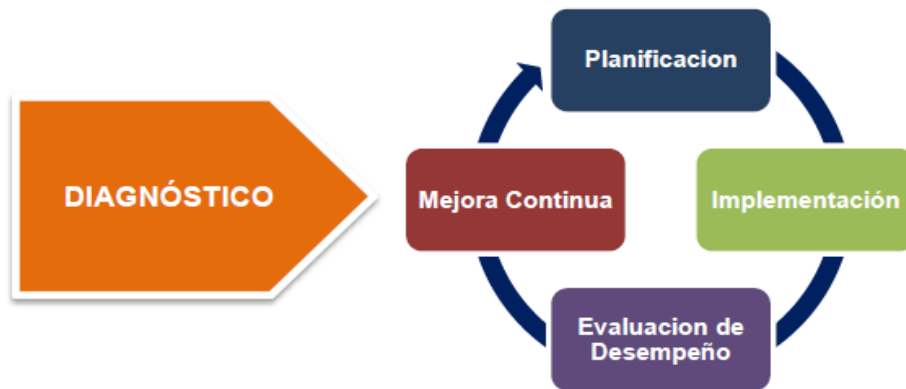


Ilustración 1Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

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

6. ACTIVIDADES PARA LA IMPLEMENTACION

1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
3. Realizar Inventario de Activos de Información con los jefes de cada oficina
4. Realizar la Valoración de los Activos de Información con los jefes de cada oficina
5. Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)
6. Socializar el Plan de Tratamiento de Riesgo
7. 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 FONCOLOMBIA

- Implementar la Política de Seguridad de la información.

Dirección: Carrera 51 #50-43 Barrio Los Cedros, Bucaramanga – Santander

Teléfono: (+57) 323 2299 720

Email: contacto@foncolombia.org.co

Horario: Lun a Vie 8:00 AM - 6:00 PM y Sab 8:00 AM - 12:00 M

- Aspectos organizativos de la seguridad de la información
- Seguridad de la Información enfocada a los recursos humanos
- Revisión de los Controles de acceso
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

8. CRONOGRAMA

No.	ACTIVIDAD	RESPONSABLE	FECHA DE IMPLEMENTACION
1	Realizar Diagnóstico	Responsable oficina TIC	Marzo de 2024
2	Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	Responsable oficina TIC	Marzo de 2024
3	Realizar Inventario de Activos de Información con los jefes de oficina	Jefes de oficina	Abril de 2024
4	Realizar la Valoración de los Activos de Información con los jefes de oficina	Jefes de oficina	Abril de 2024
5	Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)	Responsable oficina TIC	Junio de 2024
6	Socializar el Plan de Tratamiento de Riesgo	Responsable oficina TIC	Junio de 2024
7	Realizar seguimiento del Plan de Tratamiento de Riesgo	Responsable oficina TIC	Diciembre de 2024



9. SEGUIMIENTO y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con la alta dirección y el equipo de trabajo para presentar el informe de avance a la implementación del PTR y de esta manera evaluar todas las actividades propuestas en dicho plan.

10. ENTREGABLES

- Informe de avance al PTR
- Actas de Reunión.
- Plan de tratamiento de riesgo aprobado por los líderes
- Política de Seguridad
- Productos de cada etapa

Original firmado
JHON JAIRO MENESES QUINTERO
Director Ejecutivo
FONCOLOMBIA

Elaboró: Gustavo Adolfo Parada Siza
CPS-TICS