



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

“PITALEÑOS DE CORAZON”

HUGO FERNEY CASANOVA NIPI

Alcalde Municipal



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

CONTENIDO

INTRODUCCIÓN.....	2
1. PRESENTACIÓN	2
2. DEFINICIONES	2
3. OBJETIVOS	7
3.1 Objetivo General.....	7
3.2 Objetivos Específicos.....	8
4. RECURSOS	8
5. RESPONSABLES	8
6. METODOLOGÍA DE IMPLEMENTACIÓN	8
7. ACTIVIDADES	9
8. CUMPLIMIENTO DE IMPLEMENTACIÓN.....	10
9. RIESGO RESIDUAL Y DEFINICIÓN DE OPERACIONES DE MANEJO	10
10. SEGUIMIENTO Y EVALUACIÓN	12
11. ENTREGABLES	12



MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

INTRODUCCIÓN

Administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, el presente documento tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

1. PRESENTACIÓN

El presente plan se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en seguridad y privacidad de la información en la Alcaldía Municipal de El Pital- Huila, el cual busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

2. 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).

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/search?q=4140) / Código postal del municipio: [41548000](https://www.google.com/search?q=41548000)





MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

- **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.

- **Archivo**

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas**

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

- **Análisis de Riesgo**

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

- **Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- **Autorización**

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales**

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/maps/place/4140) / Código postal del municipio: [41548000](https://www.google.com/maps/place/41548000)





MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

- **Ciberseguridad**

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio**

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **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).

- **Datos Personales**

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos**

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados**

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/search?q=4140) / Código postal del municipio: [41548000](https://www.google.com/search?q=41548000)





MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Plan de continuidad del negocio**

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **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 de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada**

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/search?q=4140) / Código postal del municipio: [41548000](https://www.google.com/search?q=41548000)





MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

- **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).

- **Sistema de Gestión de Seguridad de la Información SGSI**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información**

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Trazabilidad**

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

3. OBJETIVOS

3.1 Objetivo General

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/maps/place/4140) / Código postal del municipio: [41548000](https://www.google.com/maps/place/41548000)





MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

3.2 Objetivos Específicos

- Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

4. RECURSOS

- Humano: Alcalde Municipal, Secretaria de Gobierno, Líderes de Proceso, Apoyo TIC, Técnico de Sistemas y demás Personal Externo.
- Físico: Software, Licencia de Antivirus, PC y equipos de comunicación.
- Financieros: Adquisición de Licencia de Antivirus.

5. RESPONSABLES

- Alcalde municipal
- Líderes del Proceso
- Apoyo TIC
- Técnico de Sistemas

6. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información la Alcaldía del municipio de El Pital Huila, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

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

- 1) Diagnosticar
- 2) Planear
- 3) Hacer

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/search?q=4140) / Código postal del municipio: [41548000](https://www.google.com/search?q=41548000)





MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

- 4) Verificar
- 5) Actuar

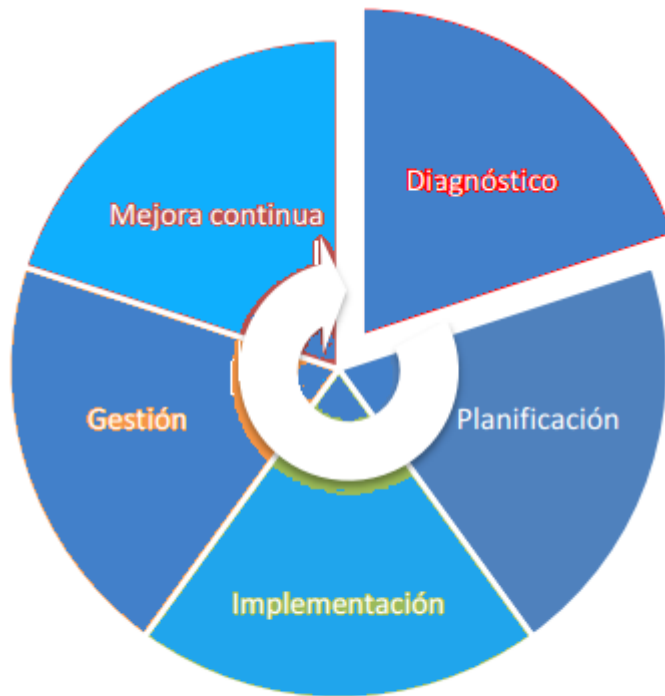


Ilustración 1 – Marco de Seguridad y Privacidad de la Información

Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

7. ACTIVIDADES

- 1) Realizar Diagnóstico.
- 2) Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- 3) Realizar la Identificación de los Riesgos con los líderes del Proceso.
- 4) Valorar el riesgo y el riesgo residual.
- 5) Realizar Mapas de calor donde se ubican los riesgos.
- 6) Plantear al plan de tratamiento de riesgo aprobado por los líderes.

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/search?q=4140) / Código postal del municipio: [41548000](https://www.google.com/search?q=41548000)





8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a 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 Apoyo TIC y el Técnico de Sistemas.

- Revisión y/o Modificación del actual Plan de Seguridad y Privacidad de la Información.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- 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.

9. RIESGO RESIDUAL Y DEFINICIÓN DE OPERACIONES DE MANEJO

Previo a la definición del riesgo residual se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control teniendo en cuenta las siguientes indicaciones:

Escala de afectación		
PROBABILIDAD	IMPACTO	AMBAS
Cuando el control está orientado a eliminar o mitigar las causas del riesgo	Cuando el control está orientado a eliminar o mitigar las consecuencias	Cuando el control elimina o mitiga causas y consecuencias del riesgo

Afectación de escalas según la probabilidad y/o el impacto

La evaluación de los controles (documentación, aplicación y efectividad) definirá la ubicación del riesgo en la matriz de evaluación; este paso se denomina “evaluación del riesgo residual”;



MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

los riesgos se pueden desplazar de la siguiente manera según la calificación de los controles y la definición de la escala que afecta cada riesgo.

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro					
Improbable					
Moderada					
Probable					
Casi Certeza					

Afectación de escalas según la probabilidad y/o el impacto

Cuando se ha determinado el riesgo residual se debe asociar la opción de manejo mediante la cual se dará tratamiento al riesgo residual. Las opciones de manejo se determinan teniendo en cuenta la ubicación del riesgo según las zonas definidas así:

Color	Zona de riesgo	Opciones de manejo
B	Zona de riesgo baja	Asumir el riesgo
M	Zona de riesgo moderada	Asumir el riesgo Reducir el riesgo
A	Zona de riesgo alta	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo
E	Zona de riesgo extrema	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: @alcaldiaelpital - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: 4140 / Código postal del municipio: 41548000





MUNICIPIO DE EL PITAL

NIT. 891.180.199-0

- **Asumir el riesgo:** aceptar la pérdida residual probable y elaborar los planes de contingencia para su manejo.
- **Reducir el riesgo:** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). Ej.: optimización de procesos, definición de nuevos controles, entre otros.
- **Evitar el riesgo:** tomar las medidas encaminadas a prevenir su materialización. Ej.: cambios a la infraestructura, cambios en software.
- **Compartir o transferir el riesgo:** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o mediante otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Ej.: seguros, sitios alternos, contratos de riesgos compartidos, etc.

10. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con la Secretaria de Despacho, Gobierno y Desarrollo Social y Apoyo TIC para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos que se han ido realizando.

11. ENTREGABLES

- Informe de avance semestral (mes de julio y diciembre).
- Acta de Reunión con Secretaria de Despacho, Gobierno y Desarrollo Social.
- Estrategias de Seguridad para la disminución de riesgos.

“Pitaleños de Corazón 2020 - 2023”

Calle 6 N° 10 – 15 Teléfono (57)(8) 8327102 - 8327050

Página Web: www.elpital-huila.gov.co e-mail: alcaldia@elpital-huila.gov.co - contactenos@elpital-huila.gov.co

Twitter: [@alcaldiaelpital](https://twitter.com/alcaldiaelpital) - Facebook: [alcaldiaelpital](https://www.facebook.com/alcaldiaelpital) / Zona Postal: [4140](https://www.google.com/search?q=4140) / Código postal del municipio: [41548000](https://www.google.com/search?q=41548000)

