

ALCALDÍA DE PASTO

SECRETARÍA GENERAL

SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN

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

|  |  |  |
| --- | --- | --- |
| ELABORACIÓN, REVISIÓN Y APROBACIÓN DE DOCUMENTOS | | |
| DATOS | AJUSTADO POR | REVISADO POR |
| FIRMA |  |  |
| NOMBRE | EDUARDO HERNÁNDEZ Z. | RAÚL ALBERTO CHAVES S. |
| CARGO | Técnico Administrativo | Subsecretario de Sistemas de Información |

CONTROL DE CAMBIOS

|  |  |  |  |
| --- | --- | --- | --- |
| No. REVISIÓN | DESCRIPCIÓN DE LA MODIFICACIÓN | FECHA DE APROBACIÓN | VERSIÓN ACTUALIZADA |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APROBACIÓN COMITÉ MIPG.

|  |  |
| --- | --- |
| NO. DE ACTA | FECHA |
| 001 | Enero-2021 |
|  |  |

# INTRODUCCIÓN

Para la Alcaldía de Pasto la seguridad y privacidad de la información es un tema prioritario que debe ser gestionado conforme a las mejores prácticas y de la mano de la estrategia de gobierno digital, para ello la entidad ha decidido implementar el modelo de seguridad y privacidad de la información propuesto por el MINTIC y de la mano de la metodología de gestión de riesgos establecida por el DAFP, que involucra riesgos de seguridad de la información se espera que de forma incremental la entidad logre proteger la confidencialidad, integridad y disponibilidad de sus activos de información y la operatividad de la infraestructura tecnológica, de tal manera que los diferentes procesos de la entidad pueden continuar su operación, en especial los procesos misionales que trabajan de la mano de la comunidad.

# DEFINICIONES

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art.3)

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. (NTC/ISO:27000)

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Información Clasificada: Es aquella información que estando en poder o custodia de un sujeto, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a ciertos derechos, contemplados en la misma ley.

Información 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).Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

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.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

# MARCO NORMATIVO

| **Norma** | **Descripción** |
| --- | --- |
| Decreto 1078 de 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. |
| Decreto 1008 de 2018 | Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. |
| CONPES 3854 de 2016 | Política Nacional de Seguridad Digita. |
| Manual para la Implementación de la Política de Gobierno Digital | Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019 |
| Modelo de Seguridad y privacidad de la información - MSPI | Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. |
| NTC / ISO 27001:2013 | Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). |
| Guía para la administración del riesgo y el diseño de controles en entidades públicas | Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre |

# OBJETIVO

Establecer las actividades que se deben desarrollar para reducir la probabilidad de la materialización de los riesgos de seguridad de la información, de la mano del modelo de seguridad y privacidad de la información propuesto por el MINTIC, las políticas de seguridad de la información, la política de protección de datos personales y la metodología de gestión de riesgos propuesta por el Departamento Administrativo de la Función Pública, alineadas a las normas técnicas ISO 27001:2013 e ISO 27002:2015.

## Objetivos Específicos

* Establecer lineamientos para unificar criterios para la administración de riesgos de seguridad y privacidad de la información.
* Adoptar el modelo de seguridad de la información propuesto por el MINTIC.
* Adoptar la metodología de gestión de riesgos propuesta por el Departamento Administrativo de la Función Pública en lo que concierne a riesgos de seguridad y privacidad de la información.
* Gestionar los riesgos de seguridad y privacidad de la información.
* Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información.
* Elaborar el mapa de riesgos de seguridad de la información de la entidad.

## Alcance

El plan de tratamiento de riesgos aplica para el proceso de gestión de tecnologías de la información.

## Plan de Tratamiento de Riesgos

# METODOLOGÍA DE IMPLEMENTACIÓN

Este plan se acoge a los lineamientos generales establecidos para la gestión integral de riesgos establecida en la Alcaldía de Pasto.

# PLAN DE TRABAJO

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Actividad** | **Producto** | **Meta** | **Fecha Inicio** | **Fecha Fin** | **Responsables** |
| Conformación equipo apoyo gestión de riesgos de seguridad de la información | Equipo apoyo gestión de riesgos de seguridad de la información conformado | Un (1) | Feb-2021 | Feb-2021 | Subsecretaría de Sistemas de Información |
| Articular la metodología de riesgos de seguridad de la Información, con metodología de gestión integral de riesgos institucional | Metodología de riesgos de seguridad de la Información, articulada con metodología de gestión integral de riesgos institucional | Una (1) | Mar-2021 | Abr-2021 | Subsecretaría de Sistemas de Información, Oficina de Planeación de Gestión Institucional |
| Sensibilización de la metodología de Riesgos de seguridad de la Información | Metodología de Riesgos de seguridad de la Información socializada | Tres (3) | May-2021 | Jun-2021 | Subsecretaría de Sistemas de Información |
| Apoyo a dependencias para la aplicación de la metodología de gestión de riesgos se seguridad de la información | Dependencias para la aplicación de la metodología de gestión de riesgos se seguridad de la información apoyadas | Diez (10) | Jul-2021 | Oct-2021 | Subsecretaría de Sistemas de Información |
| Realizar seguimiento a aplicación de metodología de gestión de riesgos en los procesos de la entidad | Seguimiento a aplicación de metodología de gestión de riesgos en los procesos de la entidad realizado | Diez (10) | Nov-201 | Dic-2021 | Subsecretaría de Sistemas de Información |