Alcaldía Municipal de Jamundí Valle del Cauca

PLAN DE TRATAMIENTO DE RIESGOS DE SPI 2022

Cra. 10 #9-74 Esquina
Tel: (052) 519 09 69
Email: oficina.tic@jamundi.gov.co
www.jamundi.gov.co – Código Postal 764001

Contenido

GLOSARIO

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 esta (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.

CGSI: Componentes de Gestión de Seguridad de la Información.

CGS-IT: Componentes de Gestión de los Servicios de Infraestructura Tecnológica.

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).

1. INTRODUCCIÓN

La Alcaldía Municipal de Jamundí – Valle del cauca, en cumplimiento de lo dispuesto en el Decreto 612 del 4 de abril de 2018 que establece: "...las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG), al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año. Teniendo en cuenta lo anterior, la Alcaldía de Jamundí "Gobierno de los ciudadanos 2020-2023", identifica los riesgos de seguridad digital y construye el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2021.

El sector público está sometido a riesgos que pueden llevar al fracaso de los procesos o incumplimiento de las metas proyectadas; por tal motivo, es necesario tomar las medidas necesarias, para identificar las causas y consecuencias de dichos riesgos. De allí, que es necesario desarrollar un análisis de riesgos de seguridad y privacidad de la información aplicado a la Alcaldía Municipal de Jamundí – Valle, realizando un diagnóstico a la infraestructura tecnológica actual, evaluando los posibles riesgos y amenazas que puedan encontrarse en la entidad y de esta manera fijar cursos de acción para implementación de medidas de protección orientadas a mitigarlos.

La Alcaldía Municipal de Jamundí Valle del Cauca, es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual deben identificar los riesgos y aplicar los controles necesarios, que garanticen la continuidad de la operación de todos los procesos administrativos.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Minimizar los riesgos asociados a los procesos tecnológicos existentes en la Alcaldía Municipal de Jamundí, con el fin de mantener a salvo los activos de información, el manejo de medios, el control de acceso y la gestión de usuarios.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar los niveles de cumplimiento y alcance de las políticas de seguridad y privacidad de la información.
- Diseñar e implementar una política integral de seguridad y privacidad de la información de en la Administración Municipal de Jamundí – Valle del Cauca.
- Establecer roles y responsabilidades para garantizar la seguridad y privacidad de la información

3. METODOLOGÍA

En la implementación del modelo de seguridad y privacidad de la información, la Entidad adopta como metodología el ciclo de planear, Hacer, Verificar y Actuar (PHVA) y los Lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los Decretos establecidos en la estrategia de Gobierno Digital.

4. ROLES Y RESPONSABILDIADES

El Comité Institucional de Gestión y Desempeño de la Alcaldía Municipal de Jamundí, velará por la implementación, aplicación, seguimiento y autorización de la política de Seguridad y Privacidad de la Información en las diferentes áreas y procesos de la entidad, además garantizará el apoyo y el uso de la política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

Este comité deberá revisar y actualizar esta política anualmente presentando las propuestas a la Alta Dirección para su análisis y respectiva aprobación.

5. GESTIÓN DE RIESGOS

5.1 Importancia de la gestión de Riesgos

La Alcaldía Municipal de Jamundí, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las entidades. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio o entidad tras sufrir alguna pérdida o daño en la información de la entidad.

Pensando en ello y la situación actual de la alcaldía Municipal de Jamundí, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios para reducir los niveles de riesgo.

6. POLÍTICA DE ADMNSITRACIÓN DEL RIESGO

La Alcaldía Municipal de Jamundí adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Con la finalidad de lograr lo anteriormente enunciado la Alta Dirección de la Administración asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política. De igual manera, el presente plan forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar su materialización.

6.1 Identificación del Riesgo

En la Alcaldía Municipal de Jamundí se contemplan las siguientes modalidades de riesgos:

Tecnológicos: Se relacionan con la capacidad tecnológica de la Alcaldía para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Imagen: Están relacionados con la apreciación y la confianza por parte de la ciudadanía hacia la Alcaldía.

Operativos: Provenientes del funcionamiento y operatividad de los sistemas de información institucional, definición de los procesos, estructura de la entidad y de la articulación entre dependencias.

Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, y el manejo sobre los bienes.

Estratégico: Se relaciona con la forma en que se administra la Entidad. El manejo de este riesgo se enfoca a asuntos generales relacionados con la misión y el cumplimiento de los objetivos estratégicos, y la definición de las políticas institucionales.

6.2 Situaciones no Deseadas

Toda Entidad busca evitar hechos que de una u otra manera atenten contra la información que allí se dinamiza. Es por ello por lo que a continuación se identifican algunas de estas situaciones que atenten contra la integridad de la alcaldía Municipal.

- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Pérdida de información.
- Baja Cobertura de internet.
- Hurto de información o de equipos informáticos.
- Alteración de claves y de información.
- Robo de información durante el horario y cumplimiento de las funciones laborales.
- Daño de equipos y de información.
- Manipulación indebida de información.
- Manipulación indebida de los equipos tecnológicos de la Alcaldía.
- Atrasos en la entrega de información.
- Perdida de información y falla de equipos tecnológicos por desastres naturales.

7. PLAN DE GESTIÓN DE RIESGOS

El ministerio de las Tecnologías de la Información y comunicación MinTIC y el Gobierno Nacional han liderado los proyectos de Gobierno Digital que permiten conocer el funcionamiento de las Alcaldías y Entidades Públicas en el país. Es por ello necesario que la Alcaldía Municipal de Jamundí cumpla con los requisitos necesarios para la entrega oportuna de la información a estas entidades, a la comunidad y a la misma Institución.

7.1 Propósito

Como propósito del plan de gestión de riesgos de la Alcaldía de Jamundí se tiene el de dar soporte al modelo de seguridad de la información al interior de la entidad, preparación de un plan de respuesta a incidentes, descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo, alcances, límites y organización del proceso de gestión de riesgos en la seguridad y privacidad de la información.

7.2 Identificación de Riesgos

Para la identificación de los riesgos de seguridad y privacidad de la información de la Alcaldía Municipal de Jamundí se tendrá en cuenta lo siguiente:

- Definición de procesos.
- Definir objetivos del proceso.
- Identificación de activos.
- Riesgo.
- Causas (amenazas y vulnerabilidades).
- Descripción del riesgo.
- Efectos de la materialización del riesgo.

8 ANÁLISIS DE VULNERABILIDADES

8.1 Diagnóstico de Vulnerabilidades

En la Alcaldía Municipal de Jamundí se encontraron las siguientes amenazas e impactos que generan incidencias en la integridad de la información, tales como:

- Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad.
- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.

Las políticas y normas de seguridad de la información serán socializadas con todo el personal, en las que se destaca:

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

Papeles reutilizables con información personal que debe ser reservada, evitando la falta de confidencialidad y privacidad.

- En algunas secretarías de la alcaldía no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.
- Algunas dependencias requieren de algunas características importantes para cumplir con las normas de funcionamiento (alimentación eléctrica estabilizada

e ininterrumpida, sistemas contra incendios, extintores, sistemas de cámaras de vigilancia, alarmas contra robo e incendios, control de temperatura y humedad entre otros.

- Existen cuentas de usuario la cuales aún no tienen protección por contraseñas para el acceso de los recursos informáticos, en equipos compartidos, los funcionarios a cargo no solicitan si desconocen de la asignación de seguridad a sus cuentas de usuario a la persona encargada de los sistemas de información e Infraestructura de TI.
- No hay control para el uso de memorias portátiles en los equipos de la Alcaldía, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
- Desconocimiento del tema de seguridad y privacidad de la información en la alcaldía.
- El sistema ofimático Microsoft Office que se utiliza en la alcaldía no cuenta con licencias de funcionamiento. Actualmente en gran parte de los equipos de la entidad está instalado Microsoft Office y no tiene licencia de uso en este caso la entidad está incumpliendo la Ley 603 de 2000.
- Los equipos computacionales no cuentan con antivirus licenciado.

8.2 Matriz de Vulnerabilidades y Mitigación de Riesgos

Anexo1: Matriz identificación de riesgos.

9. PROPUESTA DE SEGURIDAD

Según los riesgos encontrados se propone las siguientes acciones:

- Mejorar la red de cableado estructurado, para minimizar problema de acceso a la red y sus recursos compartidos, así como la conectividad de internet.
- Implementar un firewall suficiente para la red que se utiliza en la alcaldía.
- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas y dependencias.
- Formular las políticas de seguridad y privacidad de la información, con políticas de seguridad informática específicas.
- Revisar las políticas existentes para identificar debilidades y fortalezas; de ser necesario realizar los ajustes teniendo en cuenta que seguridad informática no es igual a seguridad de la información.
- Socializar las políticas de seguridad y privacidad de la información con el personal de la alcaldía.

- Establecer el procedimiento de cuentas de usuario y claves para intentar mitigar los riesgos de pérdida de información en manos de otro funcionario que use el equipo compartido.

9.1 Copias de Seguridad

Para garantizar la seguridad de la información de la Alcaldía Municipal de Jamundí debe desarrollar esfuerzos orientados a:

- Adquirir servidores con características específicas para el almacenamiento de copias de seguridad de la información local manejada en las diferentes Dependencias. [Mantener procedimientos]
- Obtener una nube dedicada para la información de la alcaldía con el fin de tener un respaldo en caso de accidentes en los equipos de cómputo. [Mantener servicio]
- Contar con un plan alternativo de energía que asegure la continuidad de la actividad en caso de que ocurran incidentes graves (tormentas eléctricas, cortes de energía). [Oportunidad de mejora]

9.2 Plan de Continuidad

- Diseñar un formato de chequeo de acuerdo con las necesidades de la organización que permita realizar las auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.
- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

  i) Detectar el riesgo
  ii) Plantear controles y efectuar las implementaciones respectivas.
  iii) Mitigar el riesgo.

10. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El análisis identificó el desconocimiento de las políticas de seguridad; por lo anterior se recomienda tener en cuenta los siguientes aspectos:

- Realizar el plan de Sensibilización de seguridad de la información y ejecutarlo cada año a toda la entidad.
- Mantener una seguridad física adecuada; lo que se refiere a todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema.

Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas, tales como:

- Detectar los requerimientos tecnológicos
- Determinar objetivos de capacitación para personal
- Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad
- Evaluar los resultados de cada actividad.

11. SEGUIMIENTO, MEDICION, ANALISIS Y EVALUACION

La Alcaldía Municipal de Jamundí evaluará el ejercicio de tratamiento de riesgos y privacidad de la información, por medio de procesos de seguimiento para verificar que las acciones se implementen, evaluando su eficiencia.

Estas actividades deberán efectuarse al menos dos (2) veces por año.

ORIGINAL FIRMADO

ANDRÉS FELIPE RAMÍREZ RESTREPO

Alcalde Municipal

Aprobó: Andrés Felipe Ramírez – Alcalde Municipal
Revisó: Valentina Moreno Viveros – Jefe Oficina
Proyectó y Elaboró: Andrés Ruiz Cadavid – Contratista TIC

Este documento fue aprobado mediante Decreto Municipal 30-16-014 del 28 de enero de 2022. Disponible en: https://www.jamundi.gov.co/Transparencia/Normatividad/DECRETO%20No.%2030-16-14.pdf