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

Contenido

1. Introducción

La información es uno de los activos más importantes de toda entidad, por lo tanto, debe estar protegida en todo momento, independientemente de la manera en que se produzca, manipule, divulgue o se almacene.
La preservación de la confidencialidad, integridad y disponibilidad de la información para la Administración Municipal de Caldas Antioquia, constituye una prioridad y por tanto, es responsabilidad de todos velar para que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. Marco Legal

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.
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.

Alineación con el Plan de Desarrollo Municipal

LÍNEA ESTRATÉGICA	COMPONENTE	PROGRAMA	PRODUCTO
Gobernanza para la transformación de la esperanza en confianza ciudadana	Transparencia, rendición de cuentas y legalidad	Gobierno digital y sistemas de información ciudadana	Acciones para Cofinanciar la modernización tecnológica de la administración municipal y las entidades descentralizadas

3. Alcance

El plan de tratamiento de riesgos de seguridad y privacidad de la información, será aplicado a los procesos estratégicos, misionales, de apoyo y de evaluación de la Administración Municipal y deberá ser conocido y cumplido por todos los funcionarios, contratistas, proveedores, ciudadanía en general y demás partes interesadas, que accedan a los sistemas de información e instalaciones físicas.

4. Direccionamiento Estratégico

Misión

La Alcaldía de Caldas, como entidad territorial, promueve y aporta al desarrollo integral para hacer de Caldas un municipio transformador, que enfrenta las diferentes formas de exclusión social, por medio del talento humano competente y con vocación de servicio, haciendo un uso adecuado y efectivo de los recursos públicos, contribuyendo a la sostenibilidad del municipio y mejorando la calidad de vida de los habitantes y de los diferentes grupos de valor.

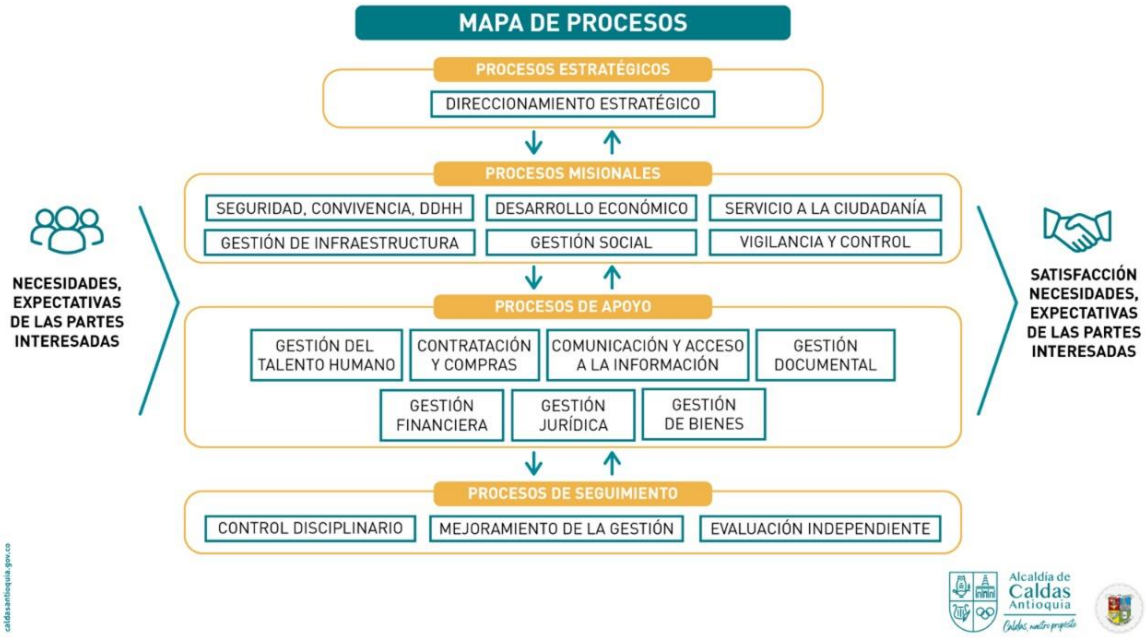
Visión

Caldas, en el año 2024, será un territorio transformado a nivel social, económico, tecnológico y ambiental, con la capacidad técnica, administrativa y operacional. Será un municipio incluyente, transparente, saludable, con un ordenamiento sostenible, al servicio del bienestar y mejoramiento de la calidad de vida de la población.

Política Sistema Integrado de Gestión

La Alcaldía de Caldas está comprometida con el mejoramiento de la calidad de vida de los habitantes del municipio, mediante la formulación y ejecución de planes, programas y proyectos que estén orientados en realizar acciones tendientes a resolver las necesidades de las partes interesadas de manera ágil y eficiente en el marco de la legalidad, transparencia e integralidad, mediante una gestión participativa, el adecuado uso de los recursos y finanzas públicas, el compromiso por el bienestar físico, mental y social de los servidores, fortaleciendo la institucionalidad y el mejoramiento continuo de los procesos, los cuales están soportados en el cumplimiento permanente de los requisitos legales.

Mapa de Procesos



5. Términos y definiciones

Con base en las herramientas facilitadas por MINTIC para la implementación de la arquitectura TI, Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina

traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional**: son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:
  - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
  - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
  - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
  - Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.
- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su

materialización. En la etapa de valoración del riesgo se determina el riesgo residual y la opción de manejo a seguir.

6. Objetivo General

Establecer y dar a conocer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información de la Administración Municipal de Caldas – Antioquia.

6.1 Objetivos Específicos

- Identificar, monitorear y hacer seguimiento a los riesgos a que está expuesta la información, con el fin de establecer metodologías que permitan una adecuada administración de éstos.
- Comprometer a todos los que tienen acceso a la información con la formulación e implementación de medidas de seguridad en pro de la prevención y administración de los riesgos.

7. Partes Interesadas

Todos los funcionarios, contratistas, proveedores, entes de control, entidades gubernamentales del orden nacional, departamental y local, y ciudadanía en general que accedan a los sistemas de información e instalaciones físicas de la Administración Municipal.

8. Desarrollo del Plan

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en el MUNICIPIO DE CALDAS - ANTIOQUIA, 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:

- Diagnosticar
- Planear
- Hacer
- Verificar
- Actuar

8.1 Plan de acción

De acuerdo con los lineamientos del Sistema Integrado de Gestión de la entidad, se debe mantener actualizado el mapa de riesgos institucional y las acciones que se definen desde informática para evitar la materialización de éstos son:

- Protección antivirus actualizada y constantemente monitoreada.
- Restricción de acceso a la información de la entidad, a través de los permisos establecidos a cada uno de los usuarios de la red interna de la Administración Municipal.
- Prohibición de instalación de aplicativos no autorizados.
- Seguridad perimetral que garantiza la protección de la red interna de la entidad, bloqueando el acceso a los sitios web dañinos, inadecuados y peligrosos que pueden contener ataques de Phishing y/o malware como spyware.
- Activación y desactivación temporal o permanente de las cuentas de usuarios de red, previa solicitud de los secretarios de despacho, jefes de oficina y/o delegados por éstos.
- Asignación o eliminación de permisos de acceso a información y/o sitios web, según se requiera.

9. Seguimiento del Plan

- Restringir los permisos de instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Administración Municipal. Está prohibida la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. Este seguimiento se hace a través de reportes generados por la plataforma de seguridad perimetral.
- Realizar back ups diarios de las bases de datos de Saimyr y QX.
- Generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando es formalmente solicitado.
- Monitorear constantemente los aplicativos de seguridad de la información, Fortinet y Antivirus, con el fin de detectar y corregir cualquier anomalía en la plataforma tecnológica de la Administración Municipal.
- Garantizar la disponibilidad de la red de datos, realizando control de tráfico y estableciendo políticas que garanticen la integridad y confidencialidad de la información. Está prohibido el intercambio no autorizado de información de propiedad de la Administración Municipal entre sus funcionarios y contratistas con terceros.