ALCALDÍA DE
FUNZA

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

VILLA IMPERIAL Y AGRICULTORA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
AÑO 2025

ALCALDÍA DE FUNZA
SECRETARÍA GENERAL
OFICINA DE RELACIONAMIENTO CON EL CIUDADANO

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

TABLA DE CONTENIDO

Contenido

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

1. INTRODUCCIÓN

El municipio de Funza, expidió el Decreto 029 del 4 de mayo de 2018, adoptando lo dispuesto en el Decreto Nacional 1499 de 2017, "por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".

De igual forma a través del Decreto Municipal 117 de 12 de diciembre del 2023, se crean las Mesas de Trabajo adscritas al Comité Institucional de Gestión y Desempeño, estableciendo su composición y se definen y adoptan las funciones específicas con el fin de asegurar la implementación, desarrollo de las políticas de gestión, directrices en materia de seguridad digital y de la información.

Lo anterior, se materializar el seguimiento a la implementación de la Estrategia de Seguridad de la Información en la Administración Municipal además de dar cumplimiento al Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", modificado por el Decreto 1008 de 2018, que dispone en el artículo 2.2.9.1.1.3., como uno de los pilares de la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Preservar la seguridad de la información es un tema que se vuelve cada día más complejo y crítico debido al uso y masificación de las tecnologías de información y las comunicaciones en las organizaciones, por esto es prioritario para la Alcaldía de Funza definir y adoptar prácticas integradas a sus procesos y operaciones, las cuales funcionan como estrategias para reducir o mitigar los riesgos de seguridad digital a los cuales se encuentran expuestos sus activos de información.

La Alcaldía mantiene la confidencialidad, integridad, y disponibilidad de los activos de información, mediante un enfoque basado en riesgos y cuyo proceso es tomado como un componente importante para el gobierno corporativo, toma de decisiones, logro de los objetivos estratégicos y cumplimiento de su misionalidad.

Un componente fundamental desde la planificación del Sistema de Gestión de Seguridad de la Información y del proceso de identificación, análisis y evaluación de riesgos de seguridad digital, es la definición e implementación de un plan de tratamiento a los riesgos, en el cual se determina implementar herramientas, sistemas, políticas, procedimientos, prácticas o mecanismos dinámicos y seguros que protejan la información y la infraestructura tecnológica que la soporta.

2. OBJETIVO GENERAL

Presentar el Plan de tratamiento de riesgos de seguridad digital identificados en la Alcaldía de Funza, el cual contribuirá al logro de los objetivos estratégicos, la visión institucional, el

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

cumplimiento de los requisitos legales y reglamentarios vigentes y aplicables, la misionalidad y la preservación de la confidencialidad, integridad y disponibilidad de la información.

3. OBJETIVOS ESPECÍFICOS

a. Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la Alcaldía de Funza podría estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
b. Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
c. Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.
d. Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información,
e. Seguridad Digital y Continuidad de la Operación

4. MARCO NORMATIVO

- NTC-ISO/IEC 27001:2022
- NTC-ISO/IEC 27001:2013
- NTC-ISO/IEC 27002:2015
- Ley 1712 de 2014
- Resolución número 00500 de marzo 10 de 2021 MINTIC Modelo de Seguridad y Privacidad de la Información
- Decreto 767 22 de mayo 2022 Política de Gobierno Digital
- Anexo 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS MINTIC 2018
- Decreto # 29 de 4 de mayo 2018
- Decreto # 117 de 12 de diciembre 2023
- Decreto 612 de 2018

5. GLOSARIO DE TÉRMINOS

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital, dentro de los cuales se puede mencionar:

- Información.
- Software.
- Recursos físicos.
- Servicios.
- Personas y sus cualificaciones, habilidades y experiencias.

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

- Elementos intangibles como la reputación y la imagen.

Activo de información: Conocimiento o datos que son de valor para la entidad. Ver modelo estándar de control interno para el Estado Colombiano, MECI 1000:2005, Numeral 2.2 Componente Información.
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).
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).
Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. 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).
Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
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).
Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
Causas: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
Control: Medida que permite reducir o mitigar un riesgo. Entiéndase por 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.
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) interacción entre usuarios.
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).

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

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).
Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
Disponibilidad: Propiedad de ser accesible y utilizable a demanda por 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)
Evaluación del riesgo: Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).
Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
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).
Identificación del riesgo: Se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.
Integridad: Propiedad de exactitud y completitud
Impacto: son las consecuencias que genera un riesgo una vez se materialice.
Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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, siempre que se trate de las 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

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

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)

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Política de administración de riesgos: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riego.

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 inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos del ambiente físico, digital y las personas.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, puede involucrar otras propiedades como como: autenticidad, trazabilidad, no repudio y fiabilidad.

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Tratamiento del riesgo: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

Valoración de riesgos: Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

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

6. ALCANCE

El Plan de Tratamiento de Riesgos, pretende realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. El Plan de Tratamiento de Riesgos definido en este documento, aplica para los riesgos de seguridad digital identificados para el proceso de apoyo Gestión de Seguridad de la Información y Recursos Tecnológicos de la Alcaldía de Funza, cuyo nivel de riesgo se encuentren en las zonas “Extremo”, “Alto”, “Moderado” y “Bajo”.

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

7. ROLES Y RESPONSABILIDADES

La Secretaría de Planeación como responsable de liderar el desarrollo e implementación del Sistema Integrado de Gestión se encargará de revisar y adecuar la metodología para la Administración de los Riesgos propuesta por el Departamento Administrativo de la Función Pública, a las necesidades de la Alcaldía de Funza, también brindará la asesoría y las herramientas a los procesos para la correcta identificación y valoración de riesgos en la entidad.

La Secretaría General será la encargada de brindar acompañamiento en el desarrollo e implementación del proceso de administración de los riesgos de seguridad digital, este deberá recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de un proceso más efectivo.

El equipo del Sistema Integrado de Gestión se encargará de recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de la metodología de Administración del Riesgo. A través de los referentes de los diferentes procesos se diligenciará el Mapa de Riesgos con el fin de registrar la gestión adelantada, así como la revisión, seguimiento y monitoreo a los riesgos y su plan de tratamiento.

El equipo de seguimiento y evaluación está conformado por Control Interno, los servidores públicos y contratistas, quienes velarán por la adecuada elaboración e implementación del mapa de riesgos de cada proceso, promoviendo su apropiación, entendimiento y evaluación del mismo.

Los responsables de implementar las acciones definidas para tratar, reducir o mitigar los riesgos de seguridad digital, se encuentran relacionados en el plan de tratamiento de cada riesgo.

8. EVALUACIÓN DEL PLAN ANTERIOR

Para la vigencia 2023 se logró 100%. De acuerdo a lo evidenciado en la Matriz consolidado Planes (Decreto 612-2018) 2023. Se adjunta LINK:

https://docs.google.com/spreadsheets/d/14CgQL2-nFDcNqJfq6Q-WIRxULIefKnc9/edit?usp=sharing&ouid=109005748311591606820&rtpof=true&sd=true

Para la vigencia 2024 se logró 93%. De acuerdo a lo evidenciado en la Matriz consolidado Planes (Decreto 612-2018) 2024. Se adjunta LINK:

https://docs.google.com/spreadsheets/d/157evamuQvA614BZut22CnoGLBTwS9kFb/edit?gid=139479918#gid=139479918

9. CONTENIDO DEL PLAN

Desarrollo del Plan - Metodología

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

Para la definición del plan de tratamiento de riesgos de seguridad digital se señalan las actividades desarrolladas previamente:

- Comprensión del contexto.
- Identificación del riesgo.
- Análisis del riesgo inherente.
- Evaluación del riego.
- Definición de controles existentes.
- Análisis del riesgo residual.
- Selección de la opción de tratamiento del riesgo.
- Definición del plan de tratamiento.

La Alcaldía de Funza, se encuentra verificando la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, y en su integración al Sistema Integrado de Gestión, por lo tanto, los riesgos identificados son los que pueden afectar la disponibilidad, integridad y confidencialidad de la información y las acciones definidas que contribuyen a la preservación de estos principios de seguridad de la información. Las medidas a implementar serán comparadas con los controles del Anexo A de la NTC-ISO/IEC 27001 a fin que no sean omitidos controles necesarios.

En el Plan de Tratamiento se determinan los siguientes ítems:

Opciones de manejo: El propósito de esta etapa es seleccionar e implementar opciones o estrategias para abordar el riesgo y con base en ella diseñar las acciones a aplicar. Las opciones para el tratamiento de los riesgos son:

- Reducir el riesgo mediante la aplicación de controles apropiados de manera que el residual se pueda reevaluar como aceptable.
- Asumir el riesgo significa que se reconoce la exposición a la pérdida, pero no se toman acciones relativas a un riesgo en particular y la pérdida es aceptada.
- Evitar el riesgo la acción que da origen al riesgo particular.
- Compartir o transferir el riesgo a entidades como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo.

Acción para tratar el riesgo: Describir las medidas o controles a implementar con el fin de lograr el tratamiento del mismo.

Soporte: Relaciona la evidencia que soportará el cumplimiento de la acción definida para tratar el riesgo.

Documentos asociados al control: Describen los documentos existentes y que de alguna manera se relacionan con la implementación del control.

Responsable: Proceso o rol encargado de la implementación y ejecución de las acciones que tratarán el riesgo.

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

Tiempo de ejecución: Fechas de inicio y terminación de la implementación de las acciones.

Indicador: Relaciona las métricas que miden la implementación de la acción.

Ver formato adjunto: MATRIZ DE INTEGRACIÓN PLANES INSTITUCIONALES Y ESTRATÉGICOS 02 - FR – 110

10. MONITOREO, SEGUIMIENTO Y EVALUACIÓN

En este apartado se describen la forma como se van a desarrollar y los recursos empleados para:

- Monitoreo: Acompañamiento continuo que el responsable del plan realiza para garantizar que se alcancen los resultados proyectados.

  El monitoreo de los planes institucionales se realiza en primera instancia por los líderes de proceso, con el objetivo de verificar el cumplimiento de las actividades establecidas en el cronograma, sugerir correctivos y acciones de mejora para realizar los ajustes y modificaciones necesarios para el cumplimiento.

  El proceso de alimentación de las actividades ejecutadas y el monitoreo cuatrimestral se realiza en formato Matriz de Integración Planes Institucionales y Estratégicos 02 - FR – 110 drive
  https://docs.google.com/spreadsheets/d/1xFL_FTMCFw5fJKFZegk1n9JBdVxJaY6n/edit?gid=139479918#gid=139479918

- Seguimiento: Análisis sistemático y periódico que permite verificar el manejo adecuado del Plan. Evaluando la congruencia de los medios empleados y los resultados intermedios con el resultado final esperado.

  La Secretaría de Planeación y Ordenamiento realizará seguimiento de manera cuatrimestral, con fecha de corte a 30 de abril, 31 de agosto y el 20 de diciembre, durante los primeros 5 días después de la fecha de corte, o con una periodicidad menor de acuerdo con las instrucciones del Líder del Proceso o jefe de la dependencia.

- Evaluación: diagnóstico crítico de los resultados obtenidos respecto a los objetivos que se perseguían, el manejo eficiente de los recursos asignados y el impacto logrado en los beneficiarios.

  La Oficina de Control Interno realizará evaluación de manera cuatrimestral, con fecha de corte a 30 de abril, 31 de agosto y el 30 de diciembre, una vez la secretaría de Planeación y Ordenamiento realice el reporte.

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

11. RIESGOS QUE PUEDEN AFECTAR EL CUMPLIMIENTO DEL PLAN

En la siguiente tabla se relacionan aquellas situaciones que potencialmente puedan llegar a producir afectaciones negativas para el desarrollo del plan y sus objetivos. Para tal efecto, se propone la siguiente tabla:

Causa Raíz	Causa Inmediata	Descripción del Riesgo	Actividades de Control	Fecha	Responsable
Falta de recurso humano	Falta de seguimiento al plan.	Posibilidad de afectación económica o reputacional por falta de seguimiento al plan.	Contar con el personal para realizar el seguimiento.	03/02/2025	Líder de Proceso

Se debe tener en cuenta que los riesgos relacionados para el plan guarden congruencia con los riesgos identificados en los procesos de la secretaría a la que pertenece.

12. APROBACIÓN, PUBLICACIÓN Y DIVULGACIÓN

El presente Plan Tratamiento de Riesgos es aprobado por el Comité Institucional de Gestión y Desempeño y estará publicado en la página web de la Alcaldía de Funza a más tardar el 31 de enero del año 2024.

Su divulgación se realizará aplicando lo establecido en la Política de Transparencia y acceso a la información pública y el Plan de Comunicaciones de la Alcaldía de Funza, así como la política de responsabilidad con la comunidad y participación ciudadana.

13. ANEXOS:

- Matriz de Integración PLANES INSTITUCIONALES Y ESTRATÉGICOS 02 - FR – 110

REFERENCIAS BIBLIOGRÁFICAS

- NTC-ISO/IEC 27001:2022
- NTC-ISO/IEC 27001:2013
- NTC-ISO/IEC 27002:2015
- Ley 1712 de 2014 Congreso de la República Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Modelo de Seguridad y Privacidad de la Información MINTIC 2021
- Resolución Número 00500 de marzo 10 DE 2021 MINTIC Modelo de Seguridad y Privacidad de la Información 2021

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

- Decreto 767 22 de mayo 2022 Política de Gobierno Digital MINTIC 2022
- Anexo 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS MINTIC 2018
- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Decreto 029 del 4 de mayo de 2018, -"Por medio del cual se adopta el decreto 1499 de 2017 para la implementación del Modelo Integrado de planeación y Gestión (MIPG).
- Decreto 080 del 25 de septiembre del 2019 por medio del cual se crean las mesas de trabajo adscritas al comité institucional de gestión y desempeño (MIPG).
- Ley 1221 de 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 0884 de 2012. Por el cual se reglamenta parcialmente la Ley 1221 de 2008.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

C.P 250020
Tel. +57(1) 823 40 70
823 40 71 / 823 40 73
Fax. +57(1) 825 76 20
Dir. Cra. 14 No. 13-05

- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- 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 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1008 del 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.
- Decreto 612 de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Resolución 2133 de 2018. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se derogan las resoluciones No 3559 y 4950 de 2013, 2313 y 494 de 2014 y 2787 de 2016.
- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

Luz Angela González Mejía
Secretario de Despacho Secretaría General

	NOMBRE DEL FUNCIONARIO	CARGO	FIRMA	FECHA
Revisó:	Sandra Milena Rosas Rojas	Jefe Oficina Relacionamiento con el Ciudadano		Enero /25
Proyectó:	Juan Pablo Guzmán	Profesional Universitario		Enero /25
Proyectó:	Erika Buitrago Ramos	Profesional Universitario		Enero /25