SECRETARÍA
TIC Y CTEI

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC) Y DE CIENCIA, TECNOLOGÍA E INNOVACIÓN (CTEI)

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

ALCALDÍA MUNICIPAL DE CAJICÁ

Ing. FABIOLA JACOME RINCON
ALCALDESA MUNICIPAL

Ing. Nicolas Castiblanco Navarrete
Secretario de TIC y CTeI
Ing. Javier Enrique Lamprea
Profesional Gobierno Digital

CAJICÁ 2024

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información MSPI, compromete la importancia de mantener la seguridad de la información y contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la Alcaldía Municipal apoyando en el uso adecuado de las TIC.

El nivel de seguridad y privacidad de la información ha sido establecido por el Gobierno Nacional en cabeza del Ministerio de Tecnologías de Información y las Comunicaciones – MinTIC para las entidades públicas a través de la Resolución 746 del 11 de marzo de 2022, "por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021". *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información como habilitador de la política de Gobierno Digital*". Es por eso que el MinTIC establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en las Entidades Públicas.

2 JUSTIFICACIÓN

Este documento "Modelo de Seguridad y Privacidad de la Información – MSPI", busca preservar la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación del proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

3 OBJETIVO GENERAL.

Implementar las actividades del Plan de Seguridad y Privacidad de la Información alineadas con la NTC/IEC ISO 27001:2013, la estrategia de gobierno digital, la Política Nacional de Seguridad Digital, CONPES 3854, en cumplimiento de las disposiciones legales vigentes.

3.1 Objetivos Específicos

· *Mantener los lineamientos establecidos para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.*

· *Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la Alcaldía Municipal de Cajicá, de acuerdo con los requerimientos establecidos en el modelo de seguridad y privacidad de la información bajo los estándares que exige la estrategia de Gobierno Digital.*

· *Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación.*

· *Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.*
· *Generar conciencia de los cambios organizacionales requeridos para la apropiación de la Seguridad y Privacidad de la Información como eje transversal de la Alcaldía municipal de Cajicá.*

· Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

4 MODELO DE SEGURIDAD MSPI

El Modelo de Seguridad y Privacidad de la Información MSPI, desde la Estrategia de Gobierno Digital contempla los siguientes ciclos de operación que contiene cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

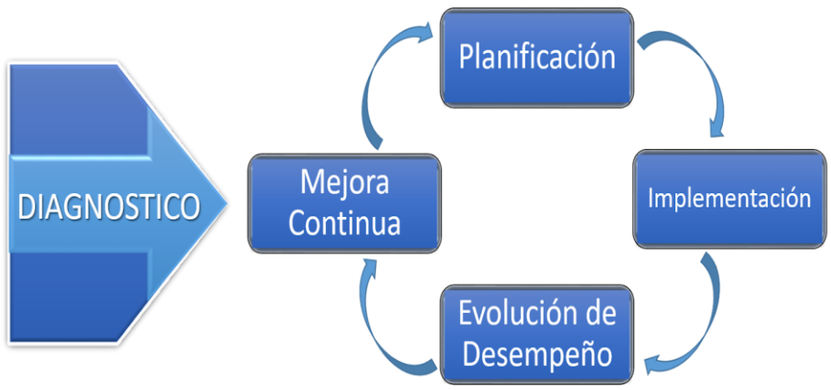


Figura 1 Ciclo de operación Modelo de Seguridad y Privacidad de la Información Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Figura 2. Fases MSPI

5 FASE DE DIAGNOSTICO

Esta Fase DIAGNOSTICO de acuerdo a la norma ISO 27001:2013, en el capítulo 4 - Contexto de la organización, determina la necesidad de realizar un análisis de las cuestiones externas e internas de la *Alcaldía municipal de Cajicá* y su contexto, con el propósito de incluir los requisitos y expectativas de las partes interesadas en la organización para lograr el alcance del SGSI.

Figura 3 Etapas previas a la implementación Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pd

5.1 Estado Actual de la Alcaldía Municipal de Cajicá

5.1.1 Conocimiento de la Alcaldía

5.1.1.1 Misión

En la Administración Municipal de Cajicá, trabajamos para cumplir las funciones que establece la Constitución Política, Leyes, Ordenanzas, Acuerdos Municipales y Decretos, para prestar los servicios públicos que nos sean asignados, realizamos gestión por resultados en aras de garantizar un territorio ordenado y sostenible, que ofrece oportunidades equitativamente sin distingo alguno en la construcción de capital humano y social, que se hace competitivo a partir de la innovación y la transformación de sus capacidades en calidad de vida y que es flexible al cambio y la mejora continua para lograr la satisfacción en sus habitantes.

5.1.1.2 Visión

Para el año 2035, Cajicá será reconocido como Municipio Modelo de Paz, referente de cierre de brechas por su equidad, inclusión, bienestar y tejido social, posicionado como líder en el contexto regional por su carácter competitivo e innovador, su alto desempeño económico y ambiental consecuente con las dinámicas de desarrollo sostenible fortalecido en su identidad y el empoderamiento de su gente.

5.1.1.3 Valores Éticos

Los Valores Éticos son las formas de ser y de actuar de los servidores públicos, son considerados altamente anhelados como atributos o cualidades propias de las personas.

HONESTIDAD: Cualidad humana que consiste en comportarse y expresarse con coherencia y sinceridad, de acuerdo con los valores de verdad y justicia. Es el respeto a la verdad en relación con los hechos y las personas.

RESPETO: Sin excepción alguna se da prevalencia a la dignidad de la persona, los derechos y libertades que le son inherentes, siempre con trato cortés y tolerante para todos los ciudadanos y compañeros.

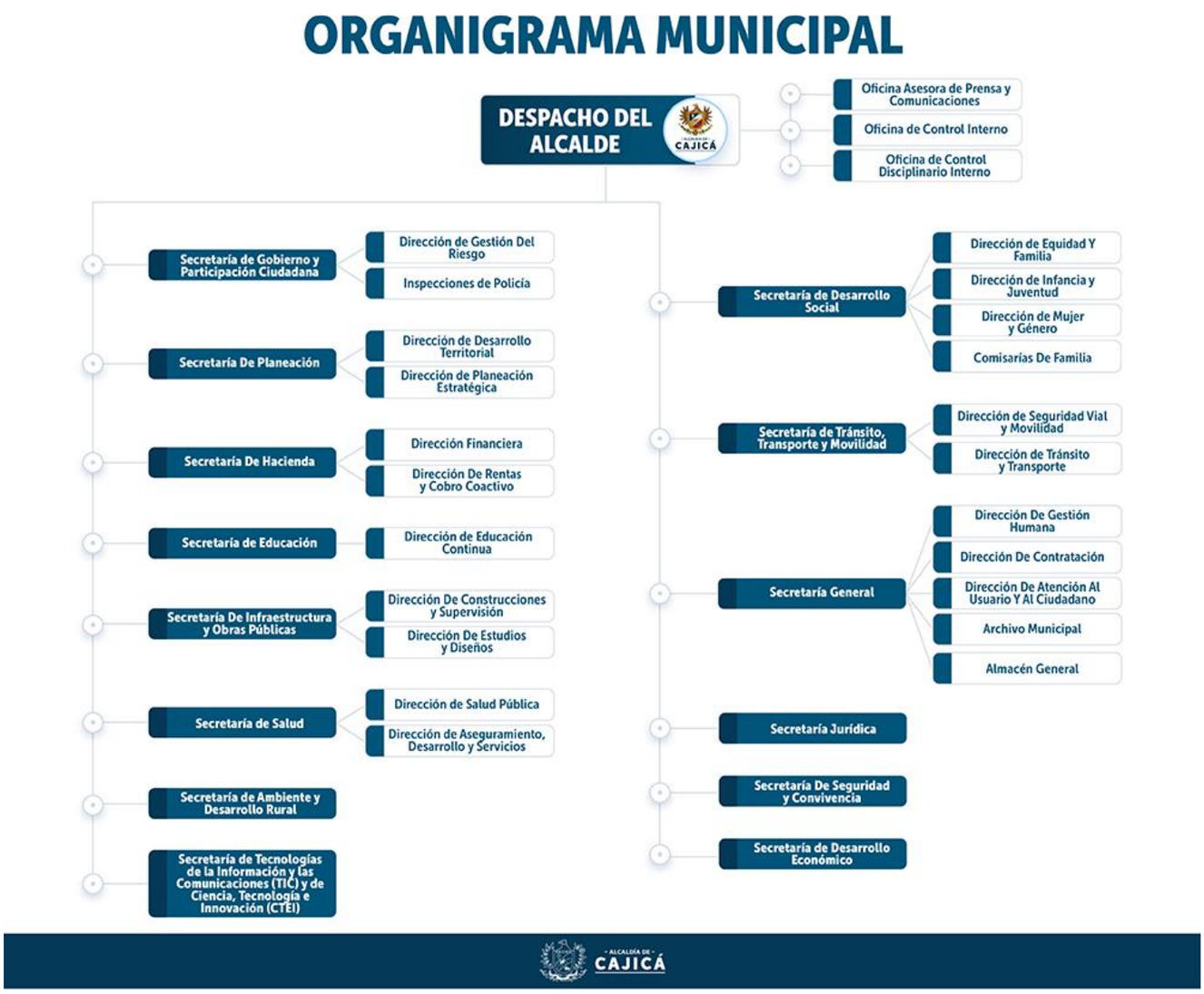
COMPROMISO: El servidor identifica y cree en la importancia de su labor la necesidad y utilidad de las funciones a su cargo.
JUSTICIA: El servidor público ceñirá sus actos a la estricta observancia de la Constitución y las leyes, así mismo sus actuaciones son ecuánimes y garantizan la equidad en el servicio.

DILIGENCIA: El servidor público desarrolla sus tareas con celeridad, pero con el cuidado necesario procurando la eficiencia en la ejecución de las mismas.

RESPONSABILIDAD: El servidor público es responsable de las acciones u omisiones relativas al ejercicio de su función, debiendo actuar con un claro concepto del deber, para el cumplimiento del fin encomendado en la entidad.

LEALTAD: El servidor público deberá guardar lealtad al Municipio, al Estado y a sus autoridades públicas, debe ser fiel a los principios éticos, buscando el cumplimiento de sus fines con plena conciencia de servicio a la comunidad y a la institución a la que pertenece. Este valor no refiere fidelidad hacia una sola persona o un grupo de poder para intereses particulares.

5.1.1.4 Organización de la Alcaldía



5.2 IDENTIFICACION DEL NIVEL DE MADUREZ

Para identificar el nivel de madurez que tiene la Alcaldía Municipal de Cajicá con respecto a la seguridad y privacidad de la información, se utilizó la herramienta “Instrumento de Evaluación MSPI de MINTIC”, el cual arrojo el siguiente resultado:

Figura 5- Niveles de madurez Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5.3 LEVANTAMIENTO DE INFORMACIÓN

Son partes interesadas de la Alcaldía Municipal de Cajicá, las entidades públicas y privadas legalmente constituidas, que interactúan con la misma; teniendo presente los requisitos normativos internos, legales o reglamentarios y las obligaciones contractuales.

PARTES INTERESADAS	DEFINICION
GOBIERNO	**MINISTERIO DE LAS TIC**
	Órganos de control, Ministerio de las Tic, Función Pública, Contraloría General de la Republica entre otras.
FUNCIONARIOS	**Funcionarios de Planta**: Personas vinculadas a la entidad bajo una relación legal y reglamentaria para el cumplimiento de funciones administrativas u otras en el marco de personal aprobada.
	Contratistas: Personas naturales que apoyan a las que trabajan en la Alcaldía de actividades del que hacer propio y misional de la Institución (Alcaldía) mediante la modalidad de prestación de servicio.
PROVEEDORES	Persona Natural, jurídica u organización que tiene vinculo contractual con la Alcaldía, para suministrar bienes, obras o servicios.

COMUNIDAD	Ciudadanos que están interesados en la misión propia de la institución.

Tabla 1 Partes Interesadas

Figura 5 mapa de procesos https://cajica.gov.co/mapa-de-procesos-2/

5.3.1 Clasificación de Activos de Información

https://cajica.gov.co/registro-de-activos-de-informacion/

6 FASE DE PLANIFICACIÓN

Esta Fase de PLANIFICACIÓN de acuerdo a la norma ISO 27001:2013, en el capítulo 5 - Liderazgo, se fija las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad que tiene la Alta Dirección de establecer una política de seguridad de la información adecuada al propósito de la Alcaldía, que asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

En el capítulo 6 – Planificación, se establecen los requerimientos para la valoración y tratamiento de riesgos de seguridad, la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el Capítulo 7 – Soporte, se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información.

Figura 6 Fase de planificación Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

6.1 Contexto de la Alcaldía Municipal de Cajicá

6.1.1 Generalidades

La Alcaldía Municipal de Cajicá, como entidad territorial que hace parte de la organización territorial de la república, goza de autonomía política, fiscal y administrativa para la gestión de sus intereses dentro de los límites de la Constitución y la Ley, y es sujeto obligado a las disposiciones que dicte el Gobierno Nacional, en lo que tiene que ver con la política de Gobierno Digital y los lineamientos dados a través del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, en lo referente a las políticas y la planeación del sector TIC.

Mediante el Modelo de Seguridad y Privacidad de la Información – MSPI se establece una estrategia integral de seguridad de la información mediante su adopción, la cual se realiza de forma integrada con el Sistema de Gestión de Seguridad de la Información, considerando que la norma ISO/IEC 27001:2013 se basa en ambos sistemas y las guías técnicas desarrolladas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, las cuales soportan transversalmente los otros componentes de la Estrategia de Gobierno Digital: TIC para el Estado y TIC para la Sociedad.

6.1.2 Contexto Tecnológico

Conectividad: La conectividad de la entidad está garantizada por un canal dedicado de Fibra Óptica que permite la interconexión con las diferentes sedes con las que cuenta la administración municipal. Esto permite que el canal de comunicación soporte las necesidades de la entidad. La Alcaldía Municipal, atendiendo a la infraestructura física, al número de sedes con que cuenta y al personal tanto de planta como contratistas que allí laboran, requiere de una arquitectura de conectividad hibrida para su funcionamiento, es decir, debe disponer de conectividad por cable e inalámbrica; así mismo respecto del Wifi, se deben definir los tipos de perfil de acceso a esta red.
Red local: La red de área local (LAN), debe garantizar que al backbone llegue la conexión dedicada en fibra y pueda ser distribuida a través de cableado al menos en categoría 5e en cada

una de las sedes. Se realizó un análisis de segmentación de acuerdo al número de sedes administrativas. Red local inalámbrica: Se realiza una revisión de la red WiFi actual para optimizar la calidad de su diseño, dentro de los cuales se debe incluir la perfilación de usuarios para su utilización y manejo. Así mismo periódicamente se realiza el cambio de contraseña.

Canal de Internet: El servicio está dimensionado para ofrecer tráfico de salida y de entrada a Internet para toda la entidad, las sedes y las Zonas Wifi. Red WIFI Comunitaria: La red Wifi comunitaria está conformada por 29 zonas Wifi distribuidas en el área urbana y rural. Cuenta con un canal de Internet de 20 MBPS distribuido para todas; a través de un radio- enlace ubicado en el sector de la Cumbre.
El servicio está dimensionado para ofrecer tráfico de salida y de entrada a internet para toda la entidad, las sedes, con un Ancho de banda de 1Gbps y para las Zonas Wifi 128 Mbps

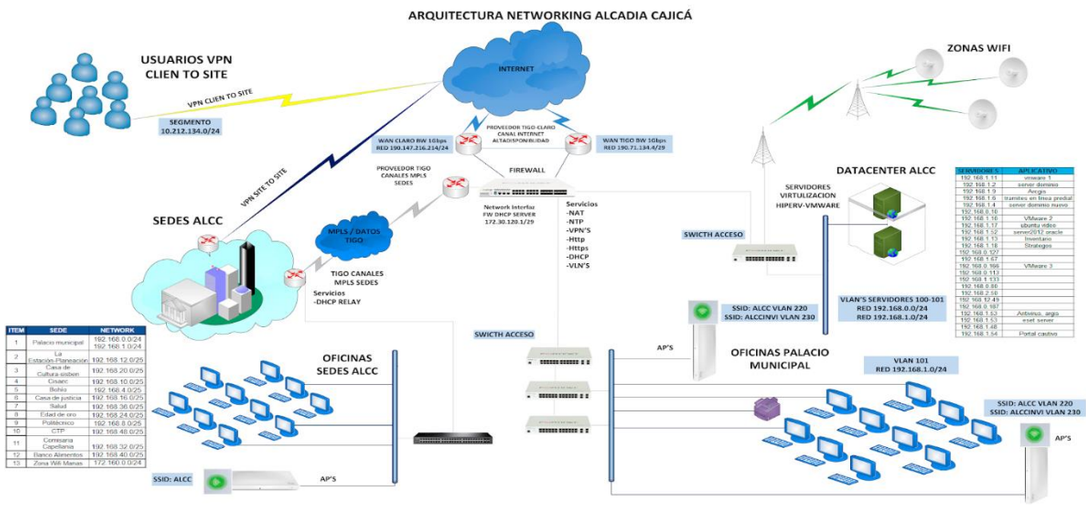


Figura 7 arquitectura networking imagen propia

6.1.3 Expectativas de las Partes Interesadas

Partes Interesadas	Necesidades	Requisitos	Solicitud	Expectativas
GOBIERNO	Contar con la información en los plazos establecidos	Cumplir con la normatividad aplicable Definir directrices y políticas ajustadas a las condiciones operacionales de la Alcaldía	Determinar las normas aplicables para el MSPI	Cumplir con los requerimientos y las directrices establecidas por los diferentes entes Gubernamentales.
				Mejorar la imagen de la institucionalidad e incrementar el nivel de competitividad
FUNCIONARIOS	Contar con herramientas tecnologías aprobadas	Apoyo tecnológico que permita seguir las directrices establecidas del SGSI	Políticas de Seguridad	Aprobación del SGSI, a través de aplicación de la políticas.
		Disponibilidad del servicio	Acuerdo de confidencialidad	Obtener Integridad y confidencialidad de la información

		Disponibilidad del servicio	Documentos del MSPII	Obtener una disponibilidad de los servicio Cumplimento de los acuerdos de nivel de servicio
PROVEEDORES	Especificaciones técnicas de lo requerido, acorde a las políticas de seguimientos del SGSI.	Cumplimiento en tiempos de entrega pactados.	Acuerdo de confidencialidad con terceros	Minimizar el riesgo del uso. inadecuado de la información
			Política de seguridad actualizada	Proteger con todo los controles de seguridad
COMUNIDAD	Información	Transparencia en el desarrollo de los procesos institucionales de la Alcaldía	Aplicar las directrices establecidas por gobierno digital	Facilitar el acceso a la información pública de manera permanente (transparencia y acceso a la información) ley 1712
		Consistencia y veracidad de la información suministrada por la institución		

Tabla 2 Expectativas Partes Interesadas

6.1.4 Alcance del MSPI

El alcance del Modelo de Seguridad y Privacidad de la Información – MSPI de la Alcaldía Municipal de Cajicá, es aplicable para todos los procesos, funcionarios, proveedores, contratistas, comunidad, y quienes, en cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten información, así como a los entes de control o entidades que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación; de esta forma buscamos proteger y preservar la integridad y disponibilidad de los activos de información.

6.2 Liderazgo

6.2.1 Liderazgo y Compromiso de la Alta Dirección

La Alcaldía de Cajicá se compromete a liderar la implementación del MSPI – Para lo cual delega la responsabilidad de la formulación, ejecución, seguimiento e implementación de los planes de mejoramiento del Modelo de Seguridad y Privacidad de la información a la Secretaria de TIC – CTeI; asignando los recursos que sean necesarios, para garantizar la seguridad de la información en la Alcaldía Municipal de Cajicá.

6.2.2 Política de Seguridad

La Alcaldía Municipal de Cajicá, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Para la Alcaldía Municipal de Cajicá, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones al rededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica. ✦ Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía Municipal de Cajicá.
- Garantizar la continuidad del negocio frente y a incidentes.
- La Alcaldía Municipal de Cajicá ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros acordes a las necesidades del negocio, y a los requerimientos regulatorios. (Min tic, 2022)

6.2.3 Roles y Responsabilidades

ROLES	RESPONSABILIDADES
Rol	Líder del Sistema de Gestión de Seguridad de la Información
Cargo	Secretario de las Tecnologías y Sistemas de Información y de las Comunicaciones - (TIC - CTeI)

Responsabilidades:

- Generar análisis y evaluación de riesgos.
- Identificación de riesgos realizada por los procesos.
- Incorporación de la gestión de riesgos.
- Identificación y evaluación de opciones para tratamiento de riesgos.
- Validar la implementación y operación del SGSI y MSPI.
- Identificación y controles para el tratamiento de riesgos.
- Implementación del plan de tratamiento de riesgos para lograr los objetivos de control identificados.
- Verificar el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Generar estudios de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable identificado.
- Definir y aplicar los procedimientos de seguimiento y revisión del SGSI.
- Generar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Generar revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Promover el desarrollo de iniciativas sobre seguridad de la información.
- Adoptar el cumplimiento y mantenimiento de registros para brindar evidencia de la conformidad con los requisitos y la operación.

6.3 PLANEACIÓN

6.3.1 Acciones para abordar Los Riesgos y Oportunidades

6.3.1.1 Identificación Valoración y Tratamiento de los Riesgos.

La Alcaldía Municipal de Cajicá realiza la identificación y evaluación de las amenazas de las vulnerabilidades relativas a los activos de información, ya sea sistemas de información, infraestructura y recurso humano, la probabilidad de ocurrencia y su impacto. Documento reservado por características de su naturaleza.

Anexo 2: Análisis de Riesgos de los Activos de Información
Documento Reservado

6.3.1.2 Plan de Comunicaciones MSPI

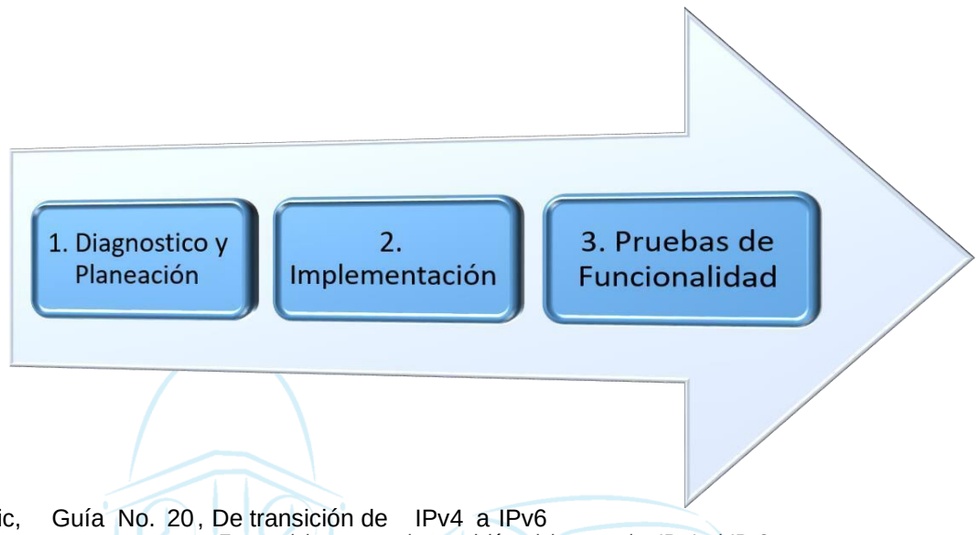
Objetivo	Que se comunica	frecuencia	Responsable	Estrategia de Comunicación	A quien se Comunica
Dar a conocerla ley 1712 de 2014 transparencia y acceso a la información pública con el fin de generar la cultura de transparencia, legalidad e integridad en la administración	ley 1712 de 2014 transparencia y acceso a la información pública y su decreto reglamentario 1081 de 2015	Anualmente	Funcionario asignado secretaria de Tic - CTeI	Página web, redes sociales, correo institucional Banner portal web	Comunidad Cajiqueña y ciudadanía en general
Dar a conocer el uso y los beneficios que plantea el Gobierno Nacional con la iniciativa de datos abiertos	Información relevante para la comunidad Cajiqueña del uso y apropiación de datos abiertos	Anualmente	Funcionarios asignados Tic - CTeI	Página Web, redes sociales, correo institucional Banner portal web, datos.gov.co	Comunidad Cajiqueña y ciudadanía en general
Socializar los procesos de gestión de recursos informáticos	uso y apropiación de recursos informáticos	anualmente / cuando se requiera	Funcionario designado Secretaria de Tic y CTeI	Inducciones funcionarios - prestadores de servicio - wallpaper pantallas institucionales - correo institucional	Personal administrativo - prestadores de servicio
Socializar información relevante relacionada con MSPI y SGSI	Tip de seguridad - seguimiento a la mejora continua	Trimestralmente - cuando se requiere	secretario y funcionario asignado de la Secretaria de Tic y CTeI	Correo inducción reinducción redes sociales institucionales talleres de gestión - wallpaper pantallas institucionales - correo institucional	Personal administrativo - prestadores de servicio

Tabla 3: Plan de Comunicaciones

6.3.1.3 PLAN DE TRANSICIÓN DE IPV4 A IPV6

De acuerdo al Modelo de Seguridad y Privacidad de la Información del Ministerio de las tecnologías, para realizar la adopción del protocolo de seguridad IPv6, se deben realizar las siguientes etapas así:

Fases de Transición a IPv6



Lineamiento Mintic, Guía No. 20, De transición de IPv4 a IPv6

Fases del proceso de transición del protocolo IPv4 al IPv6

6.4 SOPORTE

6.4.1 Recursos

Dada la importancia del Sistema de Gestión de Seguridad de la información – SGSI que hace parte del Sistema Integrado de Gestión de la Alcaldía de Cajicá, para mantenerlo en operación, hacerle seguimiento y mejora, es necesario contar con recursos económicos y humanos con las competencias específicas, la infraestructura tecnológica actualizada y el apoyo de la Alta Dirección, asignando los recursos anuales, para la adquisición y sostenimiento del mismo. En cuanto al seguimiento y mejora continua se realiza de conformidad con el procedimiento que hace parte MIPG

6.4.2 Competencias, Sensibilización y Comunicación

Competente en la elaboración, sensibilización y comunicación por la estrategia de comunicación.

7 IMPLEMENTACIÓN

Esta Fase IMPLEMENTACION en la norma ISO 27001:2013, capítulo 8 - Operación, indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

7.1 Control y Planeación Operacional

En la fase 5 de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Estado actual de la entidad, identificando el nivel de madurez de la misma, levantamiento de la información y emisión del diagnóstico.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

Para ello se recomienda utilizar los siguientes instrumentos, disponibles a través de la página web del Ministerio de Tecnologías de la Información y las Comunicaciones:

- Herramienta de diagnostico
- Instructivo para el diligenciamiento de la herramienta
- Guía No 1 - Metodología de Pruebas de Efectividad

Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

7.2 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.

El plan de tratamiento de riesgos de la Alcaldía Municipal de Cajicá se encuentra publicado en la página cajica.gov.co

web Link:

https://www.cajica.gov.co/docdown/archi/2024/Plan/PLAN%20DE%20TRATAMIENTO%20DE%20RIESGOS%20DE%20SEGURIDAD%20%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACI%C3%93N%202024.pdf.

7.3 Definición de indicadores de gestión

8 FASE DE EVALUACIÓN

La Fase EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2013 descrita en el capítulo 9 - Evaluación del desempeño, define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

Figura 9 Fase de evaluación Fuente Fase de Evaluación de Monitoreo: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

8.1 Monitoreo, Medición, análisis y evaluación

Se deben llevar a cabo actividades para realizar seguimiento a:

- La programación y ejecución de las actividades de auditorías internas del SGSI.
- La programación y ejecución de las revisiones por parte del Líder del proceso al alcance del sistema de gestión y las mejoras del mismo.
- Los Planes de seguridad tanto para el establecimiento como la ejecución y actualización de los mismos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en esta fase del SGSI
- A los registros de incidentes de seguridad que podrían tener impacto en la eficacia o el desempeño del SGSI.

8.2 Revisión por la alta dirección

La revisión por la Alta Dirección se realiza una vez al año o cuando la alta dirección lo considere pertinente, con el fin de asegurar la conveniencia, adecuación, eficacia, eficiencia y efectividad del Sistema de Gestión de Seguridad de la Información. La información presentada incluye aspectos de gestión del servicio, basados en las buenas prácticas del Estándar ISO 20000-1:2018 e ISO 27000 – 1:2013, Decreto 1581 de 2012 (por la cual se dictan disposiciones generales para la protección de datos personales. Aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.) y Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012).

9 FASE DE MEJORA CONTINUA

Esta Fase MEJORA CONTINUA en la norma ISO 27001:2013. En el capítulo 10 - Mejora, "se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan".

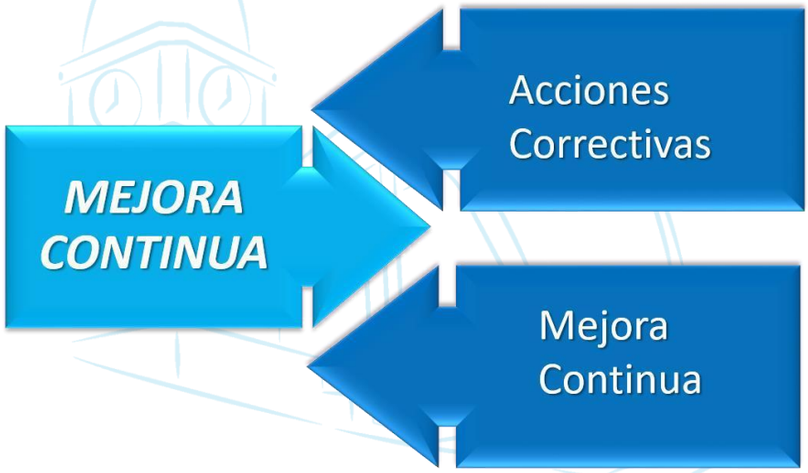


Figura 10 Fase de mejora Continua Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

9.1 Acciones correctivas

El objetivo de estas acciones es eliminar la causa de problemas asociados con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente.

- Determinar y evaluar las causas de los problemas del SGSI e incidentes de seguridad de la información.
- Diseñar e implementar la acción correctiva necesaria.
- Revisar la acción correctiva tomada.

9.2 Mejora Continua

Una vez el Sistema de Gestión de Seguridad de la Información se haya diseñado e implementado se hace necesario cerrar el ciclo con el mejoramiento continuo del mismo.

Para esto se diseña un plan de auditorías internas teniendo en cuenta el estado e importancia de los procesos y la criticidad de la información y recursos informáticos. Estos planes incluirán el alcance, frecuencia de realización, métodos de la auditoria, pruebas y selección de los auditores.

El objetivo de la auditoría interna es determinar si los objetivos de control, procesos, y procedimientos del MSPI:

- Están implementados y se desarrollan correctamente de acuerdo a los requisitos del Estándar de ISO 27001:2013.
- Cumplen los requisitos normativos.

Estas auditorías se encuentran enmarcadas dentro del procedimiento, que define las responsabilidades y requisitos para la planificación y realización de las mismas, la presentación de resultados y mantenimiento de los registros.
Además de los resultados de las auditorias, como entrada a este procedimiento se prevé también la retroalimentación de todos los participantes del SGSI y de la Alcaldía Municipal, la

revisión de los requisitos de la norma, el manejo de no conformidades, medición de los indicadores y sugerencias.

Dentro de la fase de mantenimiento y mejora se definen las acciones y se deben tener en cuenta algunas consideraciones especiales cuando se refiera a Auditorias especificas a los Sistemas de Información.

10 GLOSARIO

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, etc.) que tenga valor para la organización.

Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Amenaza informática: la aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).

Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

Autenticidad: propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Veeduría Distrital, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad. Datos abiertos: son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

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.

Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Backbone: troncal (en inglés *backbone*), red troncal o troncal de internet, es una de las principales conexiones de internet.

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Impacto: el coste para la empresa de un incidente -de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

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.

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

Parte interesada (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.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Responsable del tratamiento: 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.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

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, basando en un enfoque de gestión y de mejora a un individuo o entidad.

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.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

Política de Firewall: Una Política de Firewall es una de las herramientas más importantes a la hora de configurar un firewall, ya que a través de ciertas configuraciones que el administrador realice, según la necesidad de la empresa, se puede determinar el comportamiento del dispositivo en la red.

11 TABLA DE ILUSTRACIONES

12 TABLA DE TABLAS

13 REFERENCIAS

Mintic. (25 de 04 de 2022). *mintic.gov.co*. Obtenido de mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad_____MS