PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA MUNICIPAL DE CAJICÁ

DIRECCIÓN TIC´S - CTeI

CAJICÁ 2022

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

GLOSARIO

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la información (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000)

Administración de Riesgos: Conjunto de Elementos de Control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.

Confidencialidad: la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados

Evaluación del Riesgo: Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos ubicados en los niveles: Nivel bajo, moderado, alto y extremo y fijar prioridades de las acciones requeridas para su tratamiento.

Integridad: la propiedad de salvaguardar la exactitud e integridad de los activos.

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

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

Evento de seguridad de la información: una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

1. INTRODUCCIÓN

Para la Alcaldía de Cajicá es de gran importancia que el talento humano que presta sus servicios conozca de manera clara los riesgos asociados a la seguridad y privacidad de la información. Adicionalmente que cuente con los recursos tecnológicos apropiados para prevenir y mitigar los incidentes que se puedan presentar.

De esta manera, podremos trazar y diseñar un plan de comunicación mucho más eficaz y adaptado a las necesidades específicas de la Alcaldía de Cajicá.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

La implementación del plan de Seguridad y Privacidad de la Información en la Entidad está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

2. OBJETIVO

Diseñar una estrategia de apropiación del Plan de Seguridad y Privacidad de la Información para la Alcaldía de Cajicá.

Este documento busca describir las actividades del plan de seguridad y privacidad de la información con base en el modelo PHVA (Planear-Hacer- Verificar-Actuar) definido en la norma ISO 27001, identificando en cada fase las actividades a realizar dentro de la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI) en el marco del modelo de referencia definido por el Ministerio de Tecnologías de la Información – MINTIC-MSPI y en concordancia con el Modelo Integrado de Planeación y Gestión -MIPG adoptado en la Entidad.

POBLACIÓN OBJETIVO

La Plan de Privacidad y Seguridad de la Información está dirigido al personal de la Alcaldía de Cajicá, tanto de la planta de personal como los contratistas.

3. DOCUMENTO DE REFERENCIA

- Decreto 103 de 2015 el cual reglamenta la ley 1712 de 2014 "Ley de Transparencia “.
- Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, “Protección de datos personales”.
- Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.
- ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de Información.

4. ALCANCE PLAN MSPI

Establecer la hoja de ruta para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI que es aplicable a todos los procesos de la Entidad; funcionarios, contratistas, lo cual comprende las políticas, procesos, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información.

5. OBJETIVO PLAN MSPI

Establecer las actividades contempladas en el MSPI alineadas con la norma técnica ISO 27001, definir acciones lineamientos necesarios para fortalecer la seguridad de la información y garantizar la disponibilidad, integridad y confidencialidad de esta dentro de la Entidad, a partir de las definiciones dadas por el Modelo de Seguridad y Privacidad de la Información - MSPI, la norma técnica ISO 27001 y el Modelo Integrado de Planeación y Gestión- MIPG.

6.1 Objetivos Específicos Plan MSPI

- Definir, actualizar, excluir controles o elementos normativos para proteger la información de la Entidad frente a los criterios de confidencialidad, integridad y disponibilidad.
- Implementar la metodología de Administración y Gestión de Riesgos con el fin de mitigar el impacto en una posible materialización de un riesgo.
- Implementar el plan de comunicaciones del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información fortaleciendo la Entidad.
- Adelantar revisiones del Sistema de Seguridad de Información con el fin de verificar el funcionamiento de este
- Definir los procesos para mejora continua del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información.
- Fortalecer los procedimientos relacionados al Modelo de Seguridad de la Información.
- Dar cumplimiento a la normatividad vigente en materia de Seguridad y Privacidad de la Información.

6. EL MODELO PHVA

El Sistema de Gestión de la Seguridad de la Información (SGSI) inmerso dentro del MSPI, se basa en la necesidad que la Seguridad de la Información esté en continua evolución y que, además, dicha evolución esté documentada y justificada. El modelo en el que se basa el SGSI es denominado PHVA (Planear-Hacer-Verificar- Actuar). La Ilustración 1 representa la relación entre las fases del modelo y los numerales de la norma ISO 27001

6.1 PLANEAR

En esta primera fase se realiza un estudio de la situación actual de la Alcaldía de Cajicá, desde el punto de vista de la seguridad de la información, es necesario estimar las medidas que se van a implementar en función de las necesidades detectadas, determinando así el alcance del MSPI y la política de seguridad.

Se debe tener en cuenta que no toda la información de la Alcaldía de Cajicá tiene el mismo valor en cuanto a los tres pilares (Confidencialidad, integridad y disponibilidad), e igualmente, no toda la información está sometida a los mismos riesgos. Por ello, una de las actividades importantes dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así mismo, se hace necesario el análisis de dichos riesgos con el fin de evaluar los posibles impactos para la Entidad y con base en ello, establecer planes de acción con miras a mitigar dichos riesgos.

6.1.1 Contexto de la Organización

En general, esta fase consiste en entender el contexto de la Alcaldía de Cajicá como entidad que garantiza la prestación de los perfiles definidos dentro de su misionalidad, apoyándose en su visión, en su estructura jerárquica, en sus sistemas de información y en sus partes interesadas, e identificar los requisitos y expectativas de la seguridad de la información desde la perspectiva del cumplimiento de los requerimientos de usuario o parte interesada. Para ello es importante comprender los procesos y procedimientos en los que se soporta para cumplir sus objetivos, mirar el contexto interno y externo de la Entidad, definir los flujos de información con cada una de las partes interesadas y en general, comprender a la entidad como un Sistema, dando como resultado el entendimiento de la Entidad y a partir de eso, la definición del alcance del Sistema de Seguridad de Información, los objetivos del MSPI y la Política general de seguridad de la información.

6.1.2 Políticas de Seguridad de la Información

La Alta Dirección apoyada en el Comité Institucional de Gestión y Desempeño buscará establecer controles administrativos y operativos, que regulen de manera efectiva el acceso de los usuarios de los sistemas a nivel de aplicación, sistema operativo, bases de datos, red y acceso físico.

Teniendo en cuenta lo anterior se adopta el Manual de las políticas de Seguridad de la Información de cumplimiento por parte de directivos, funcionarios, usuarios y terceros que accedan a la información de la Entidad, usen equipos informáticos y de comunicaciones, interactúen con herramientas tecnológicas y/o servicios informáticos y/o ingresen de manera física o lógica a las instalaciones de la Unidad.

La ruta en la página web es la siguiente:
https://cajica.gov.co/transparencia-y-acceso-a-la-informacion-publica/ ,
https://cajica.gov.co/politicas-institucionales/ realizar clic en Políticas de Seguridad de la Información.

Se elabora el documento Políticas de Seguridad de la Información para dar cumplimiento con algunos controles del anexo A de la norma ISO 27001 de acuerdo con los lineamientos ahí definidos y mediante la resolución 589 de 2019 "Por la cual se adopta la Política de Seguridad de la Información de la Alcaldía de Cajicá

La ruta en la página web es la siguiente:
https://www.cajica.gov.co/docdown/archi/2019/Resolucion/Resoluci%C3%B3n%20No.%20110%20de%202018.PDF

6.1.3 Identificación y Clasificación de Activos de Información

Un activo de información, según la ley 1712 de 2014, es el elemento de información que la Unidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio

electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

Las actividades a realizar para obtener un inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información:

6.1.3.1 Definición

Los activos de información que se gestionan en todos los procesos de la Entidad deben cumplir con lo siguiente:

- Número consecutivo único que identifica al activo en el inventario.
- Proceso al que pertenece el activo.
- Propietario / Responsable
- Custodio.
- Nombre del activo de información.
- Descripción del activo de información.
- Categorización del activo de información: por ejemplo, hardware, software, servicio, personas, la cual debe revisarse periódicamente o cuando se presenten cambios en la información o en la estructura que puedan afectarla.
- Idioma.
- Medio de conservación.
- Periodicidad o de generación o actualización en caso de activos expedientes físicos y digitales.
- Condición legitima de la excepción (Ley 1712 transparencia y Ley 1581 tratamiento de datos).
- Fundamento constitucional o legal.
- Descripción de Condición legitima de la excepción.
- Clasificación del activo de acuerdo a la ley de transparencia.
- Valoración del activo (confidencialidad, integridad y disponibilidad).

6.1.3.2 Revisión

El inventario de activos puede ser revisado o validado en cualquier momento que se requiera y por lo menos debe revisarse y actualizarse una vez al año, con el fin de validar el estado del activo, el proceso al que pertenece, cambio o aumento de actividades, desaparición de un área o proceso, cambios o migraciones de sistemas de información del proceso entre otros.

6.1.3.3 Actualización

Cuando el propietario del activo o el líder del Proceso defina alguno de los cambios mencionados anteriormente en los activos de información, se debe actualizar el inventario de activos de información.

6.1.3.4 Publicación

La Entidad, determina que el inventario de activos de información es un documento clasificado como “Público”, sin embargo, aquellos activos de información que por su carácter reservado y que son de naturaleza sensible a los procesos estratégicos de la Entidad, serán clasificados como “Confidenciales”, por lo cual no serán publicados.
El líder de cada proceso será el responsable del inventario de activos de seguridad de la información y las modificaciones que se requieran solo se deben hacer previa autorización del Oficial de Seguridad de la Información o quien haga sus veces.

La ruta en la página web es la siguiente:
https://cajica.gov.co/transparencia-y-acceso-a-la-informacion-publica/#

6.1.4 Análisis de Brecha

El análisis de brecha busca generar un diagnóstico relativo a la seguridad de la información basado en la identificación de diferencias entre el estado actual y el estado ideal de la Unidad Administrativa Especial de Servicios Públicos de acuerdo con los requerimientos exigidos en la norma ISO 27001:2013, el Modelo de Seguridad y Privacidad de la Información - MSPI y las consideraciones definidas internamente como parte del ejercicio de la Entidad y el cumplimiento de su misionalidad.

Las fases para realizar una metodología de diagnóstico de seguridad de la información son:

- Revisión del cumplimiento de las exigencias de la Norma ISO 27001 en concordancia con el modelo de seguridad y privacidad de la Información - MSPI, respecto a la Seguridad de la Información, la gestión de los riesgos, el análisis de vulnerabilidades y el seguimiento a las mismas.

- Revisión de los controles existentes que apliquen a la seguridad de la información en la Alcaldía Municipal de Cajicá según el anexo A de la citada Norma.

- Identificar requisitos faltantes (Políticas, procedimientos, controles), los cuales son exigidos por la norma ISO 27001 y por el modelo del MinTic – MSPI.

En cumplimiento con lo establecido por el MINTIC, se va a usar la herramienta de autodiagnóstico de seguridad y privacidad de la información elaborada por ellos, la cual arroja un resultado que permite a cada entidad visualizar los diferentes dominios de la norma, evaluar las falencias y a partir de eso, generar un plan de seguridad de la información para ser desarrollado al interior de la misma y dar cumplimiento con lo estipulado en el manual de gobierno digital en sus diferentes componentes.

6.1.5 Documentación de Procedimientos

Durante esta fase se identificarán y documentarán procedimientos necesarios para dar cumplimiento a la norma ISO 27001 y a las necesidades propias que la entidad requiere, garantizando un adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información - MSPI. Actualmente el proceso de Gestión Tecnológica y de la Información cuenta con los siguientes procedimientos dentro del Sistema Integrado de Gestión:

- Procedimiento para la Formulación y Ejecución Plan de Tecnologías de la Información (PETI)
- Procedimiento Mantenimiento Preventivo de Equipos
- Procedimiento de Mesa de Ayuda y Mantenimiento Correctivo Plataforma Tecnológica
- Procedimiento de Administración de Hardware

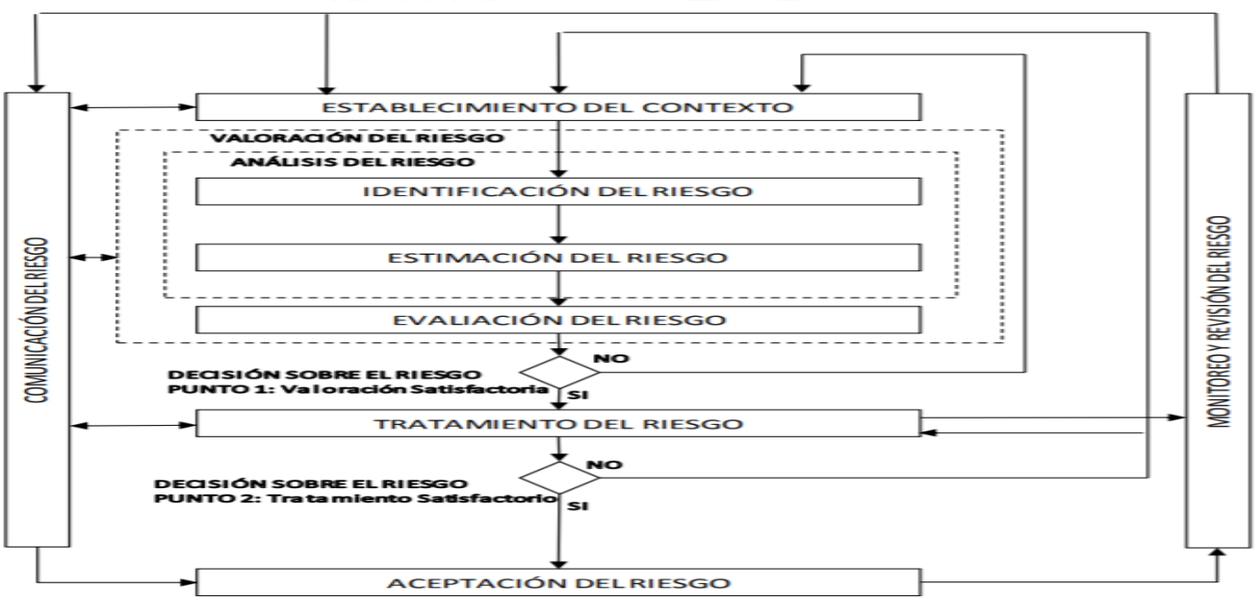
- Procedimiento de Administración Sistemas de Información y Software
- Procedimiento de Administración de Comunicaciones
- Procedimiento de Administración de Servidores
- Procedimiento Administración de Copias de Seguridad
- Procedimiento para el Sistema General de Seguridad de la Información
- Procedimiento Administración Cuentas de Usuario
- Procedimiento Activos de Información

Cabe aclarar que todos los procedimientos se encuentran en revisión y actualización con forme con a las necesidades y la dinámica de la Dirección de TIC´s - CTeI .

6.1.6 Metodología para la Gestión de Riesgos

La gestión de riesgos de seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento, el cual es adoptado desde la Oficina Asesora de Planeación como Política de gestión de Riesgos y el SGSI – MSPI se une a dichos dictámenes que acoplan el Modelo de Riesgos definidos por el Departamento Administrativo de la Función Pública – DAFP a la Entidad. En ese sentido y de forma ilustrativa, se visualiza el siguiente gráfico con el fin de esquematizar de manera somera el proceso descrito por la entidad:

Ilustración 1. Administración del riesgo en seguridad de la información



Fuente: NTC-ISO/IEC 27005

Así como lo ilustra la imagen anterior, la gestión del riesgo es iterativo para las actividades de valoración del riesgo y/o el tratamiento de este. Un enfoque iterativo para realizar la valoración del riesgo incrementa la profundidad y el detalle de la valoración en cada iteración y obliga a un proceso de mejora continua como se está proponiendo dentro de este sistema.

La gestión de riesgos ofrece un método sistemático para analizar los riesgos derivados de los procesos y del uso de las tecnologías de la información y comunicaciones,

con el objetivo de descubrir y planificar el tratamiento oportuno, mantener los riesgos bajo control y así preparar a la entidad para un proceso de evaluación, auditoría, certificación o acreditación, según corresponda.

6.1.7 Programas de Sensibilización y/o Formación de Empleados

El documento ***Plan de Sensibilización*** presenta la planeación para realizar el programa de sensibilización y/o formación sobre Seguridad de Información dentro de la Entidad, el cual tiene como objetivos principales, lograr que los miembros (funcionarios y contratistas) que integran la Alcaldía Municipal de Cajicá, entiendan y se comprometan con todos los aspectos relacionados con el Sistema de Gestión de Seguridad de la Información, a partir de la creación de una cultura relacionada con la integridad, confidencialidad y disponibilidad de la información, en donde todos los miembros de la entidad comprendan la importancia de dar un tratamiento adecuado a la información y finalmente concientizar a las personas de los riesgos que se pueden presentar tanto para ellas como parte integral de la Alcaldía y su misión social.

6.1.8 Gestión de los Recursos del SGSI-MSPI

Es compromiso de la Dirección de la Alcaldía municipal de Cajicá, garantizar los recursos tanto presupuestales como del talento humano para la implementación exitosa del SGSI - MSPI.

6.1.9 Soporte

6.1.9.1 Recursos

La Alta Dirección con el apoyo de la Oficina de Tecnología de la Información y las Comunicaciones deben planificar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información.

6.1.9.2 Competencia

La competencia significa la capacidad con la que se aplican los conocimientos y las habilidades en la Entidad con el fin de conseguir los resultados previstos en cuanto a la implementación del Sistema de Gestión de la Seguridad de la Información.

A continuación, se describen las siguientes competencias:

PERFIL	COMPETENCIAS
	1) Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión - MIPG. **2)** Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión - MIPG. **3)** Proponer al Comité Sectorial de Gestión y el Desempeño Institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG.

Comité Institucional de Gestión y Desempeño	**4)** Presentar los informes que el Comité Sectorial de Gestión y el Desempeño Institucional y los organismos de control requieran sobre la gestión y el desempeño de la entidad. **5)** Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión. **6)** Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. **7)** Las demás que tengan relación directa con la implementación, desarrollo y evaluación del Modelo.
Jefe de TIC	**1)** El jefe de TIC tiene la responsabilidad global del suministro y uso de las TIC en la Entidad. **2)** Debe Organizar y supervisar el trabajo de un equipo de personas especializadas que son las encargadas de diferentes tareas en cuanto a la implementación y seguimiento del SGSI-MSPI. **3)** Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
Encargado de Infraestructura (Profesional de Servidores)	**1)** Garantizar la definición, monitoreo, accesibilidad, funcionalidad y mantenimiento de las redes y servidores del Entidad. **2)** Colaborar en la correcta ejecución y control de los procesos de creación de respaldos de información y/o recuperación. **3)** Registrar y controlar el inventario de infraestructura de la de la Dirección de Tecnologías de Información y Comunicación. **4)** Supervisar el correcto funcionamiento de la plataforma tecnológica de la Entidad a través de sistemas de monitoreo, a fin de prevenir interrupciones en el servicio y gestionar las acciones que permitan garantizar su adecuado funcionamiento.
Dirección TIC´s - Ctei	**1)** Respetar y seguir las normas y procedimientos definidos en la política de seguridad de la información. **2)** Notificar al responsable de seguridad de la información las anomalías o incidentes de seguridad, así como las situaciones sospechosas. **3)** Mantener la confidencialidad, integridad y disponibilidad de la información. **4)** Hacer un buen uso de los activos de información de la Entidad.

6.1.9.3 Toma de Conciencia

La Oficina de Tecnologías de información y las Comunicaciones, adelantará un plan de sensibilización y/o formación por diferentes medios, buscando que todos y cada uno de los funcionarios, contratistas y partes interesadas, se enteren de la implementación del MSPI-SGSI, sus pormenores y sobre todo de la labor que cada uno de ellos adelanta dentro de la entidad, haciendo especial énfasis en las responsabilidades de cada uno y los posibles problemas que recaen sobre ellos o la entidad, en el caso del incumplimiento de las políticas de Seguridad de Información.

6.1.9.4 Comunicación

La entidad tiene definido un procedimiento para manejo de incidentes de seguridad, el cual plantea actividades específicas orientadas a la comunicación de dichos incidentes a las partes interesadas.

6.1.9.5 Información Documentada

La Entidad, dentro de la implementación del MSPI-SGSI, adelantará el registro y documentación de los requerimientos exigidos por la norma ISO27001:2013 y los documentos adicionales definidos por el MSPI, llevando a cabo el versionamiento solicitado por la norma y alineado a los procedimientos definidos por la oficina de Planeación para llevar a cabo este tipo de tareas.

6.2 HACER

6.2.1 Operación

En esta fase se lleva a cabo el establecimiento de los controles de seguridad escogidos en la fase anterior junto con los seguimientos, actualizaciones y procesos de mejora propios. Dentro de esta fase se destaca el cumplimiento del plan de sensibilización, que conlleva a la concientización y/o formación del personal de la Alcaldía municipal, de cara a que conozcan los controles implantados, el rol que cada funcionario, contratista o parte interesada desempeña y, sobre todo, el buscar la colaboración de cada una de las personas como parte activa del sistema.

Dichos controles se especifican en el documento **Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información.**

6.2.2 Gestión de Funcionamiento normal del MSPI

La Alcaldía de Cajicá debe adoptar el Sistema de Gestión de Seguridad de la Información SGSI-MSPI, como parte integral y trasversal de la Entidad y como tal, debe gestionar las operaciones del Sistema mediante el seguimiento y revisión continuo de todo el sistema, la evaluación y toma de decisiones frente a los resultados definidos por las métricas e indicadores adoptados y generando planes de mejoramiento para optimizar los resultados y suplir las falencias encontradas, todo esto confluyendo en auditorías internas y externas que demuestren la fortaleza o no del sistema desarrollado.

6.2.3 Gestión de Incidentes de Seguridad

La Alcaldía de Cajicá implementará un ***Plan de Gestión de Incidentes,*** creado para detectar y gestionar un incidente, definido como toda aquella actividad ejecutada como resultado de eventos adversos e inesperados que ocurran como resultado de controles fallidos o inexistentes, teniendo en cuenta las directrices adelantadas por MINTIC, la Policía Nacional y los entes competentes en esta área.

6.3 VERIFICAR

6.3.1 Evaluación de Desempeño

La Alcaldía de Cajicá dispone de mecanismos que le permitan evaluar la eficacia y éxito de los controles implementados. Por este motivo toman especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del MSPI.

- Implementa procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos y determinar si las actividades de seguridad se desarrollan de acuerdo con lo previsto.
- Revisa periódicamente la eficacia del MSPI mediante la evaluación y análisis de las métricas definidas para tal fin.
- Revisa periódicamente el estado de los activos de información, actualizando periódicamente la matriz correspondiente y la matriz de riesgos

- Revisa periódicamente la evaluación de riesgos, actualizando el Plan de tratamiento de riesgos.
- Realiza Auditorías internas planificadas.
- Adelanta revisiones por parte de la alta dirección para asegurar el funcionamiento del MSPI para identificar oportunidades de mejora.
- Actualiza los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión en el caso que sea necesario.
- Mantiene registros de las actividades e incidentes que puedan afectar la eficacia del MSPI.

6.4 ACTUAR

6.4.1 Mejora Continua

En esta fase se llevarán a cabo las labores de mantenimiento y mejora del sistema de gestión de seguridad de información, seguimiento a riesgos, análisis de vulnerabilidades, hacking ético, así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se puede llevar en paralelo con la verificación y se despliega al detectarse la deficiencia o hallazgo negativo, no esperando a adelantar una fase de verificación programada para comenzar con las tareas de mejora continua y corrección.

- Implementa y documentación en el MSPI las mejoras identificadas.
- Toma medidas correctivas y preventivas y aplica las mejores prácticas sobre incidentes de seguridad, provenientes de experiencias de seguridad propias y de terceros documentadas.
- Comunica las actividades y mejoras a todos los grupos de interés.
- Busca que las mejoras cumplan los objetivos previstos y que estén enfocadas a las necesidades y requerimientos de la Entidad.

7 PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se realiza su respectivo.

CANALES DE COMUNICACIÓN

El Plan de Seguridad y Privacidad de la Información será difundida a través de los siguientes mecanismos, estará, se diseñarán piezas publicitarias para que sean publicadas a través del fondo de escritorio de los equipos de cómputo de la Alcaldía de Cajicá (Cuentas de Dominio), los chat institucional y correo electrónico.

CANAL	ACTIVIDAD	RESPONSABLE
Talleres de Sensibilización	Se realizarán talleres en cada una de las dependencias, teniendo en cuenta los espacios concertados con los funcionarios.	Dirección de TICS-CTel
Página Institucional	Publicar en la página de la Alcaldía de Cajicá www.cajica.gov.co el Plan de Seguridad y Privacidad de la Información en las secciones de: Transparencia y Acceso a la Información Pública. Planes y Políticas, MIPG y Dirección TICS.	Dirección de TICS-CTel

Fondo de escritorio, chat institucionales y correo electrónico.	Difundir las piezas publicitarias	Dirección de TICS-CTel / Oficina de Prensa y Comunicaciones

PLAN DE ACCIÓN

Para realizar la difusión del Plan de Seguridad y Privacidad de la Información se tendrá en cuenta el siguiente cronograma de actividades:

FASE	ACTIVIDADES	MES (2022)				RESPONSABLE
		Feb	Mar	Abri	Jun	
Preparación	Diseño de piezas publicitarias					Oficina de Prensa y Comunicaciones
	Diseño y aprobación de metodologías para los talleres de sensibilización					Dirección de TICS-CTel

Implementación	Difusión a través de los canales de comunicación					Dirección de TICS-CTeI
	Concertación de Cronograma para los talleres.					Dirección de TICS-CTeI
	Realizar los talleres de sensibilización					Dirección de TICS-CTeI
Seguimiento y Evaluación	Análisis de las experiencias recogidas en los talleres de sensibilización.					Dirección de TICS-CTeI

GESTIÓN	ACTIVIDADES	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS
Documentación MSPI.			
	Actualizar y aprobar el Plan de Sensibilizaciones del MSPI.	Oficina TIC.	30/01/2022.
	Actualizar la Declaración de aplicabilidad (SOA).	Oficina TIC.	31/08/2022.
	Actualizar los Procedimientos, Instructivos, Manuales con relación al MSPI.	Oficina TIC.	31/12/2022.
	Revisar los lineamientos para el levantamiento de activos de información.	Oficina TIC.	30/01/2022.
Relación con proveedores/ transferencias de información.	Definir los Acuerdos de confidencialidad con proveedores y terceros.	Oficina TIC/ - Contratación .	30/06/2022.
Gestión de riesgos Riesgos	Identificar y gestionar Riesgos de Seguridad de la Información.	Oficina TIC.	31/12/2022.

de Seguridad de la Información.	Realizar el Seguimiento a la Matriz de Riesgos de Seguridad de la Información.	Oficina TIC.	31/12/2022.
Seguridad de las Operaciones	Apoyar en las Auditorías Internas y Externas al MSPI.	Oficina TIC.	31/12/2022
Indicadores MSPI	Formular, Implementar, actualizar y reportar los indicadores del MSPI.	Oficina TIC.	31/12/2022
Protección de datos personales	Actualizar la Política para el tratamiento de Datos Personales.	Oficina TIC.	1/07/2022
	Registrar y actualizar las bases de datos personales ante la Superintendencia de Industria y Comercio-SIC.	Oficina TIC.	1/07/2022.