PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019

FUNDACIÓN GILBERTO ALZATE AVENDAÑO

GESTIÓN TIC.

Contenido

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información expuestos en este documento, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27001 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

2. AUDIENCIA

Funcionarios de carrera, provisionales, contratistas de la Fundación Gilberto Alzate, así como proveedores de servicios que contractualmente se encuentren o vayan a realizar algún tipo de vinculación con la entidad deben conocer y adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

Este documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información.

La fundación Gilberto Alzate Avendaño es la entidad encargada de promover las artes plásticas, visuales, escénicas, musicales, literarias y audiovisuales, así como de la participación y formación democrática a través de debates, foros, seminarios y cátedras, así mismo debe adoptar y promover las políticas, planes, programas y proyectos del sector cultura, es así como a través de la Estrategia de Gobierno en Línea se debe adoptar también los concerniente a las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

El Modelo de Seguridad y Privacidad de la Información – MSPI, lleva a la protección de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

4. JUSTIFICACIÓN

La fundación Gilberto Alzate Avendaño a través de la Subdirección de Gestión Corporativa dando cumplimiento a sus funciones, contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

5. GLOSARIO

Acceso a la Información Pública
Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

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

Activo de Información
En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

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)

Amenazas
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).

Auditoría
Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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)

Bases de Datos Personales
Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

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).

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

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)

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)

Declaración de aplicabilidad
Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la

justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

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).

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)

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).

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 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)

Ley de Habeas Data
Se refiere a la Ley Estatutaria 1266 de 2008.

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

Mecanismos de protección de datos personales
Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio
Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

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.

Registro Nacional de Bases de Datos
Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada
Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos
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. (Ley 1581 de 2012, art 3).

Riesgo
Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información
Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Tratamiento de Datos Personales
Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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. (ISO/IEC 27000).

Vulnerabilidad
Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. OBJETIVOS

6.1 OBJETIVO GENERAL

Crear un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la Fundación Gilberto Alzate.

6.2 OBJETIVOS ESPECÍFICOS

- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas para la Fundación Gilberto Alzate.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Apoyar en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- Optimizar el acceso a la información pública al interior de la entidad.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

7. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que la entidad pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, y los servicios tecnológicos que permiten que la entidad funcione observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

8. DESCRIPCIÓN DEL CICLO DE OPERACIÓN

A continuación se entra en detalle con respecto funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de la Fundación Gilberto Alzate Avendaño.

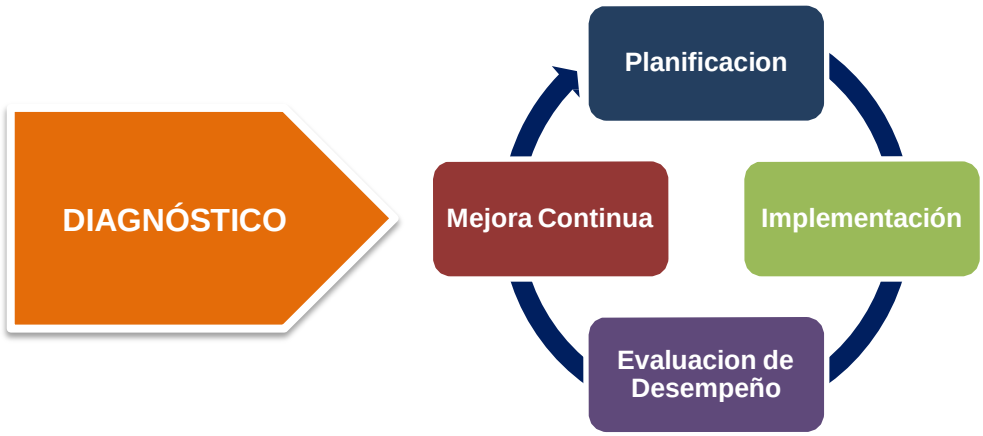

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

8.1 FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Tabla 1 - Metas, Resultados e Instrumentos de la fase etapas previas a la implementación:

Metas	Resultados	Instrumentos MSPI
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico

En la fase 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.
- 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.

8.2 FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

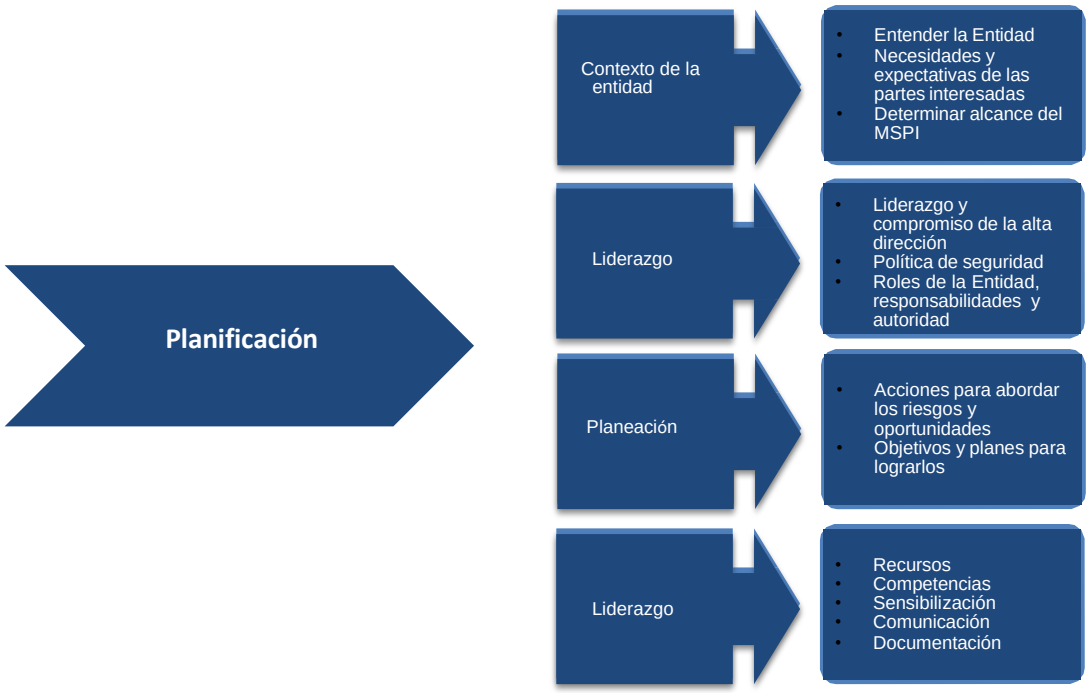

Figura 3 - Fase de planificación[1]

Tabla 2 - Metas, Resultados e Instrumentos de la Fase de Planificación

Planificación		
Metas	**Resultados**	**INSTRUMENTOS MSPI**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI

[1] El contenido de la figura 3 fue tomada de la Norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar como se desarrolla la planificación del MSPI.

Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía no 2 - Política General MSPI
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestion Documental
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	Guía No 7 - Gestion de Riesgos Guía No 8 - Controles de Seguridad
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación

A continuación se expone de manera general la fase de planificación del Modelo de Seguridad y Privacidad de la Información.

Política de seguridad y privacidad de la información.
La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

Políticas de Seguridad y Privacidad de la Información.
Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información
En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente.

Procedimientos de Seguridad de la Información.
En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.

Roles y Responsabilidades de Seguridad y Privacidad de la Información.
La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

Inventario de activos de información.
La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

Integración del MSPI con el Sistema de Gestión documental.
La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.

Identificación, Valoración Y Tratamiento de Riesgos.
La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos.

Plan de Comunicaciones.
La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.

8.3 FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

Tabla 3 - Metas, Resultados e Instrumentos de la Fase de Implementación

Metas	Resultados	MSPI
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadores de Gestión SI.

Con base a los resultados de la fase de planeación, en la fase de implementación deberá ejecutarse las siguientes actividades:

Planificación y Control Operacional.

La Fundación Gilberto Alzate Avendaño debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

Implementación del plan de tratamiento de riesgos.

Se debe implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad.

Indicadores De Gestión.

La entidad deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.
Los indicadores buscan medir:

- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumo al plan de control operacional.

8.4 FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Tabla 4 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

Metas	**Resultados**	
		MSPI
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16 – Evaluación del desempeño.
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 15 – Guía de Auditoría.

Plan de revisión y seguimiento a la implementación del MSPI.

En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI
- Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

Plan de Ejecución de Auditorias

La entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

8.5 FASE DE MEJORA CONTINUA

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

Tabla 5 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Metas	Resultados	MSPI
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua

En esta fase se define y ejecuta el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, la entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad.

9. MODELO DE MADUREZ

Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentra la entidad, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado.

Tabla 6 – Características de los Niveles de Madurez

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad. • No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. • La entidad cuenta con un plan de diagnóstico para IPv6.

Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información • La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad

Fecha	Versión	Razón del cambio
21/01/2019	1	Versión inicial

Elaboró:	Revisó y aprobó:	Verificación SIG :
Edwin Gustavo Díaz Méndez Profesional Contratista TIC	Licette Moros León Subdirectora de Gestión Corporativa	Sonia Córdoba Asesor Planeación