VIGILADA MINEDUCACIÓN

PROFESIONAL

Ruta de la calidad

Capacitamos para la Transformación Productiva

PLAN DE SEGURIDAD DE LA INFORMACIÓN (PSI)

2022-2025

Por

MARIO GERMÁN CALDAS MARTÍNEZ

IT4+

Modelo de Gestión de Tecnologías de la Información – TI.

El futuro digital es de todos

Gobierno de Colombia MinTIC

GUSTAVO ADOLFO RUBIO LOZANO
Rector

CLAUDIA XIMENA TRIANA VERA
Vicerrector Académico

DARÍO ALFONSO PAYÁN SANCLEMENTE
Asesor

Guadalajara de Buga, Valle del Cauca
2023

Tabla de contenido

Lista de tablas.

Lista Ilustraciones

Lista Anexos

Abreviaturas y acrónimos

Abreviatura	Significado
AAC	Acreditación de Alta Calidad
AE	Arquitectura Empresarial
AI	Arquitectura de Información
AMP	Acuerdo Marco de Precios
ANS	Acuerdos de Niveles de Servicio
ATI	Arquitectura de la Tecnología de la Información
BCP	Plan de Continuidad del Negocio - Business Continuity Plan
BPM	Business Process Model and Notation (Notación y modelamiento de procesos de negocios)
CIO	Chief Information Officer - director o Jefe de Tecnologías de la Información.
CMMI	Integración de modelos de madurez de capacidades - Capability Maturity Model Integration
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas - Control Objectives for Information and related Technology
CONPES	Consejo Nacional de Política Económica y Social
CT+I	Ciencia, Tecnología e Innovación
DAFP	Departamento Administrativo de la Función Pública
DNP	Departamento Nacional de Planeación
EPCA	Encuesta de Percepción Ciudadana sobre Calidad y Accesibilidad de Trámites y Servicios
ESP	Programa de Estrategia Empresarial (Enterprise Strategy Program)
GTIC	Grupo de Tecnologías de la información y las Comunicaciones

I+D	Investigación y Desarrollo
IGC	Índice Global de Competitividad
INC	Informe Nacional de Competitividad
IT4+	Modelo de Gestión Estratégica de Tecnologías de la Información
ITA	Instituto Técnico Agrícola
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información - Information Technology Infraestructure Library
MGPTI	Modelo de Gestión de Proyectos
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
MIPG	Modelo Integrado de Planeación y Gestión
MRAE	Marco de Referencia de Arquitectura Empresarial
MSPI	Modelo de Seguridad y Privacidad de la Información
NOC	Network Operations Center, Centro de Operaciones de Redes
OCDE	Organización para la Cooperación y el Desarrollo Económico
PEI	Plan Estratégico de Tecnologías de la Información
PETI	Plan Estratégico de las Tecnologías de Información y las Comunicaciones
PMBOK	Guía de los Fundamentos de Gestión de Proyectos - Guide to the Project Management Body of Knowledge, es un libro de estándares, pautas y normas para la gestión de proyectos.
PMI	Project Management Institute
PMO	Oficina de Gestión de Proyectos - Project Management Office
PND	Plan Nacional de Desarrollo
PQRS	Peticiones, Quejas, Reclamos y Solicitudes.
PSI	Plan de Seguridad de la Información
RGC	Reporte Global de Competitividad
RPO	Punto de Recuperación Objetivo - Recovery Point Objective
RTO	Tiempo de Recuperación Objetivo - Recovery TIme Objective
SGSI	Sistema de Gestión de la Seguridad de la Información
SOC	Centro de Operación de Seguridad - Security Operation Center
TI	Tecnologías de la Información
TIC	Tecnología de la Información y las Comunicaciones

Definiciones

Término	Definición
Actividades	Acciones a desarrollar en una institución de manera cotidiana, como parte de sus obligaciones, tareas o funciones.
Análisis de Riesgos	Es el uso sistemático de la información disponible para determinar la frecuencia para determinados eventos donde se pueden producir y la magnitud de sus consecuencias.
Aplicaciones	Es un programa informático diseñado como una herramienta para realizar operaciones o funciones específicas
Arquitectura	Según ISO/IEC 42010: Proceso de concebir, expresar, documentar, comunicar, certificar la implementación, mantener y mejorar la arquitectura a través de todo el ciclo de vida de un sistema

Arquitectura Empresarial	Es una práctica estratégica (una capacidad), consiste en analizar integralmente las empresas desde diferentes perspectivas o dimensiones (el negocio, la información, las aplicaciones, la infraestructura), con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria.
Arquitectura Misional o de Negocio	Describe los elementos de una institución, le permiten implementar su misión. Esta arquitectura incluye el catálogo de servicios misionales; el modelo estratégico; el catálogo de procesos misionales, estratégicos y de soporte; la estructura organizacional, y el mapa de capacidades institucionales.
Cadena de valor	Relación secuencial y lógica entre insumos, actividades, productos y resultados donde se añade valor a lo largo del proceso de transformación total.
Caracterización de proceso	Representación esquemática de un proceso, permite conocer su objetivo, alcance y sus principales actividades del ciclo PHVA.
Ciclo PHVA	El ciclo de Deming, también conocido como círculo PDCA corresponde al acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), Ciclo de mejoramiento continuo.
Mapa de Ruta	El principal entregable de la arquitectura empresarial es el mapa de ruta. Después de evaluar el estado actual (AS-IS) y establecer la situación objetivo donde se quiere llegar (TO-BE),
Arquitectura de TI	Describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).
Generar Valor	Proveer un conjunto de servicios y productos para facilitarle a un cliente el logro de un objetivo. La generación de valor es donde los clientes perciban los beneficios de una iniciativa de arquitectura.
Dato	Un dato por sí mismo no constituye información ni conocimiento, como mínimo requiere una interpretación para poder generar conocimiento y/o información; pero también podría requerir el procesamiento de otros datos y/o metadatos para ser generador de información
Dominio	Cada uno de los seis componentes de la estructura de la primera capa del diseño conceptual del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.
Eficacia	Grado en el cual se realizan las actividades planificadas y se alcanzan los resultados planificados.
Eficiencia	Relación entre el resultado alcanzado y los recursos ejecutados
Extracción de Datos	Es el proceso de colección de datos de un sistema de acuerdo con los requerimientos detallados en una especificación funcional. Este proceso puede requerir desarrollo, pruebas y ejecución de programas en uno o varios sistemas.
Flujos de información	Corresponde a la descripción explicita de la interacción entre proveedores y consumidores de información a lo largo de un proceso o patrón repetible de invocación definido por parte de la Institución.
Gestión de riesgos	Es un enfoque estructurado para manejar la incertidumbre relativa a las amenazas o factores de riesgo susceptibles afectar el cumplimiento de los objetivos, buscando disminuir la probabilidad y el impacto de su

	materialización. Incluye las actividades de identificación, evaluación, tratamiento y, seguimiento y mejora de la eficiencia de los controles.
Gestión de la Tecnología	Permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas. (MinTIC, 2015)
Gobernabilidad	Define la capacidad de una organización para controlar y regular su propio funcionamiento con el fin de evitar los conflictos de intereses relacionados con la división entre los beneficiarios y los actores.
Gobierno de TI	"El Gobierno TI es un conjunto de procedimientos, estructuras y comportamientos utilizados para dirigir y controlar la organización hacía el logro de sus objetivos" (www.iteraprocess.com, s.f.).
Gobierno Digital	Es la estrategia de Ministerio de las TIC, busca construir un Estado más eficiente, más transparente y participativo gracias a las TIC.
Información	Unidad básica de conocimiento. Es un conjunto de datos organizados y procesados los cuales Tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades.
Infraestructura	Conjunto de elementos lógicos y físicos permiten una determinada solución funcione adecuadamente, tal y como fue diseñada.
Interoperabilidad	La interoperabilidad es la acción, operación y colaboración de varias entidades para intercambiar información, permite brindar servicios en línea a los ciudadanos, empresas y otras entidades mediante una sola venta de atención o un solo punto de contacto. Es decir, es la forma de ahorrarle a la gente los desplazamientos de un lugar a otro a la hora de realizar un trámite y de hacer el proceso menos engorroso.
Marco de Referencia de Arquitectura Empresarial	Es el instrumento principal, la carta de navegación, para implementar la Arquitectura TI de Colombia. Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información
Plataforma	Es un sistema, sirve como base para hacer funcionar determinados módulos de hardware o de software compatibles.
Producto	Son los bienes y servicios, se obtienen de la transformación de los insumos a través de la ejecución de las actividades.
quick wins o "victorias rápidas"	Son una herramienta profesional para conseguir resultados de una forma rápida y con una inversión generalmente baja dentro de una empresa
Resultados	Son los cambios en las condiciones del sujeto de beneficio enmarcadas en el objetivo general del proyecto, por efecto del consumo de los productos y el cumplimiento de los supuestos considerados en el mismo.
Riesgo	Efecto de la incertidumbre sobre los objetivos. (ICONTEC, 2011)
RPO Recovery Point Objective	Se refiere al volumen de datos en riesgo de pérdida, los cuales la organización considera tolerable. ¿Las transacciones de cuánto Tiempo se está dispuesto a perder, o a reintroducir al sistema?
RTO Recovery TIme Objective	Expresa el Tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.
Servicios de TI	Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficiente implementación de las capacidades institucionales. A través de la prestación de estos servicios TI, se produce valor

	a la organización. Los servicios de información son casos particulares de servicios de TI.
Servicios Digitales	Permiten a los grupos de interés interactuar con otros sistemas de información de la entidad, del sector, del Estado y con el ciudadano; consumiendo y proporcionando información, a través de servicios disponibles en la web, en un modelo estructurado de portales de información
Sistemas de Información	Es un conjunto de elementos orientados al tratamiento y administración de datos, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
Sistemas de Información Misionales	Soportan la misión de la entidad, procesando de manera eficaz las transacciones del negocio, actualizando bases de datos, controlando procesos operativos, generando documentación del negocio y recopilando información sectorial, entre otras responsabilidades, las cuales dependen del Tipo de misión de la Institución.
Transparencia	De acuerdo con la Corporación Transparencia por Colombia (2010), la transparencia es el "marco jurídico, político, ético y organizativo de la administración pública", las cuales regir las actuaciones de todos los servidores públicos en Colombia, implica gobernar expuesto y a modo de vitrina, al escrutinio público.

Derechos de Autor

Introducción.

Se adoptó la concepción, metodología, lineamientos e instrumentos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), las cuales conforman la ESTRATEGIA DE GOBIERNO DIGITAL, soportada en los lineamientos para la elaboración del MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) y el PLAN DE SEGURIDAD DE LA INFORMACIÓN (PSI).

El Instituto Técnico Agrícola (ITA), hace parte de las entidades públicas del Estado Colombiano, es consecuente con la realidad donde las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la comunidad y como tal, cumplidor de las política de gobierno digital, cuyo objetivo es promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las Entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Institución enmarcados en su modelo de operación por procesos.

El Instituto Técnico Agrícola (ITA), como responsable de la implantación y desarrollo de Modelo de Seguridad y Privacidad de la Información (MSPI), así como la de establecer su reglamentación, entre las cuales se encuentra "Las políticas de gestión y directrices en materia de seguridad digital y de la información", pero también con el objetivo de orientar a la Institución para dar cumplimiento con lo solicitado en el Decreto 612 de 2018, "por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado" y todas las consideraciones expuestas, dentro de las cuáles se encuentra el Decreto 1078 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" y los instrumentos para implementar la Estrategia de Gobierno en Línea (Ahora Gobierno Digital), dentro de los cuales se exige la elaboración por parte de cada entidad, de un Plan de Seguridad y Privacidad de la Información.

El Decreto 1083 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", donde se establece lo siguiente: "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción (artículo 74 de la Ley 1474 de 2011), deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…) 12. Plan de Seguridad y Privacidad de la Información".

La Institución teniendo en cuenta la anterior fundamentación, coloca en conocimiento mediante este documento el proceso de implementación y socialización del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), articulado con la política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión (MIPG) y las disposiciones de la ley 1581 de 2012, "por el cual se dictan disposiciones generales para la protección de datos personales", el Decreto 1377 de 2013 "por el cual se reglamenta parcialmente la Ley 1581 de 2012" (se dictan disposiciones generales para la protección de datos personales) y el Decreto 886 de 2014 "por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".

La seguridad de la información, según ISO/IEC 27001:2013, consiste en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de Gestión de Riesgo, (ISO/ IEC 27001 Versión 2013), para lo cual, el proyecto busca dar respuesta a las exigencias del Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, (MinTIC), para todas entidades públicas.

Se debe tener en cuenta, el Plan de Seguridad de la Información (PSI) contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la Institución apoyada en el uso adecuado de las TIC y a su vez es un componente transversal a la Estrategia de Gobierno en línea, permitiendo el alineamiento a los siguientes componentes:

- TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, contribuya al cumplimiento de la misión y los objetivos estratégicos de la entidad.
- TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios ofrecidos por la Institución, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley, exceptúa el acceso público a determinada información.

- TIC para Gobierno Abierto, permite la construcción de un estado más transparente, colaborativo y participativo al garantizar una información proveedora de controles de seguridad y privacidad de tal forma, los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

Por consiguiente, la Institución establecerá un Plan de Seguridad de la Información (PSI) como un proceso para garantizar la efectividad de los controles definidos para la custodia de los activos, vele por una información correcta y completa, esté siempre a disposición del cumplimiento de las metas de la institución y esté respaldada y sea utilizada sólo por aquellos autorizados para hacerlo, y una actualización de plazos anuales, cuáles serán las labores realizadas por la Institución con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos.

1 Objetivos

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información (MSPI), alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos de la IES Instituto Técnico Agrícola (ITA)

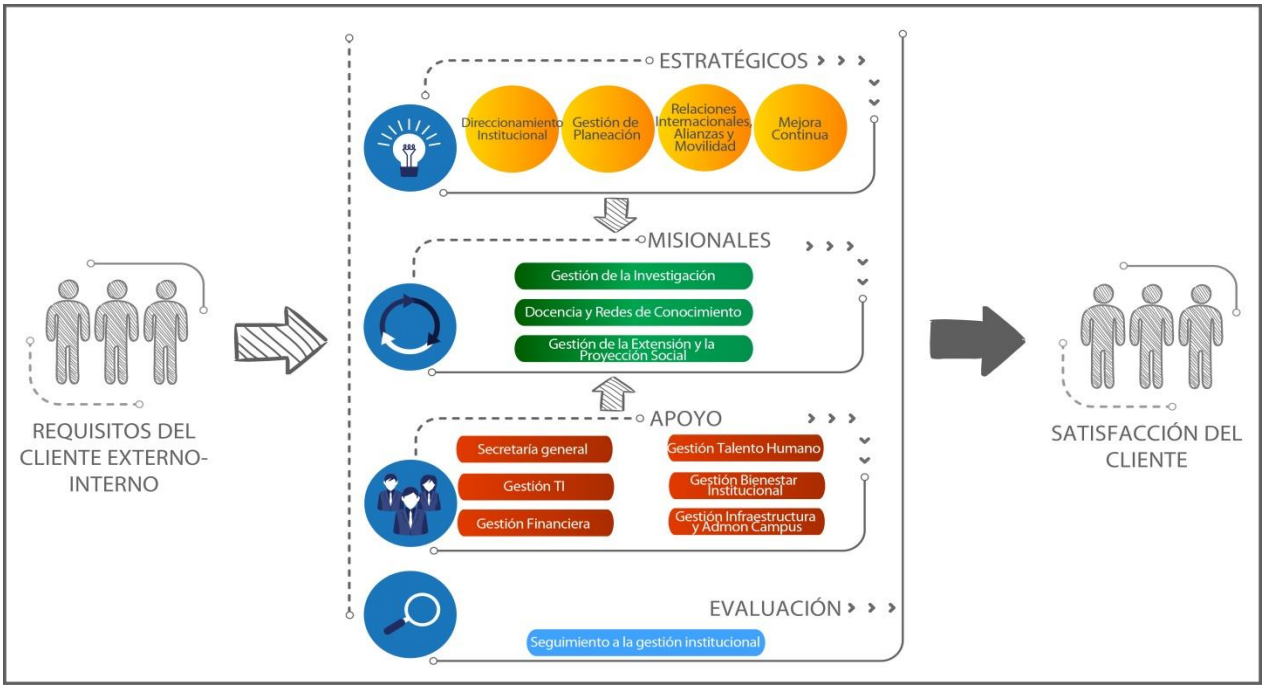


Ilustración 1. Mapa de Procesos de la IES Instituto Técnico Agrícola (ITA)
Fuente: Tomado página web institucional ITA.

1.1 Objetivo general.

Definir las actividades (hoja de ruta)contempladas en el Modelo de Seguridad y Privacidad de la Información - MinTIC, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos y así, liderar y establecer las estrategias para la gestión de seguridad y privacidad de la Información en la Institución, implementando y evaluando acciones efectivas en procura de la mejora continua y de la salvaguarda de la información, permitiendo minimizar los riesgos de pérdida de activos de la información y estando alineadas a la estrategia y al Sistema Integrado de Gestión (SIG) y acordes con las necesidades institucionales y los lineamientos del programa de Gobierno Digital.

1.2 Objetivos específicos.

Se define los objetivos del PSI, y así, cumplir con los siguientes criterios específicos, medibles, alcanzables, importantes en la Institución y con Tiempos definidos. Los objetivos están alineados con los objetivos estratégicos de la Institución y con los objetivos sectoriales y/o territoriales según aplique.

Tabla 1. Objetivos específicos

Descripción de objetivo
Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables, facilitando de manera integral la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital y continuidad de la operación de los servicios.
Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal, al definir, operar y mantener el Plan de Continuidad de la Operación de los servicios dela Institución.
Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información de la Institución, definiendo los lineamientos necesarios 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.
Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.
Implementar proteger los activos de información de la Institución, con base en los criterios de confidencialidad, integridad y disponibilidad, con acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno Digital, definiendo, reformulando y formalizando los elementos normativos sobre los temas de protección de la información.

Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, para mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.
Sensibilizar a los servidores públicos y contratistas de la Institución acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Institución.

Fuente: Construcción propia.

2 Alcance.

Identifica la metodología, documentos y procesos, los permiten a la Institución desarrollar el Plan de Seguridad y Privacidad de la Información aplicado para todos los procesos de la Institución, a todos los funcionarios, contratistas y demás colaboradores, en cumplimiento de sus funciones utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas con acceso a la información, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, este plan aplica para toda la información creada, procesada o utilizada en la Institución sin importar el medio, formato, presentación o lugar en el cual se encuentre, precisando las fases de su implementación y sus tareas macro; garantizando de esta forma el tratamiento de la información utilizada en los trámites y servicios ofrecidas por la Institución, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley, exceptúa el acceso público a determinada información.

3 Marco normativo.

Para el desarrollo del Modelo de Seguridad y Privacidad de la Información (MSPI) y del Plan de Seguridad de la Información (PSI), se deben tener en cuenta las normas vigentes: externas, tales como las disposiciones legales y la normatividad vigente expedida por las autoridades; y las internas, tales como los decretos y las resoluciones de la organización. La proliferación de disposiciones sin la evaluación de impacto y la previa revisión de viabilidad a su expedición por el área de TI, genera dificultades en la implementación y complicaciones, por lo tanto, los sistemas de información se "adapten", a veces sin éxito práctico, a las modificaciones y a los requerimientos.

El Estado Colombiano ha determinado las normas por las cuales se rige la gestión y administración de la Seguridad y Privacidad de la Información especialmente en las entidades públicas.

Tabla 2.Normatividad de la gestión y administración de los servicios de las TIC

Marco normativo	Descripción
Constitución Política de Colombia1991 - Artículo 15	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones,
Decreto 103 de 2015,	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1377 de 2013	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1494 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 2573 de 2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 2609 de 2012.	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Decreto 4632 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Ley 1273 de 2009,	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 1474 de 2011	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014;	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Ley 23 de 1982	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

Ley 527 de 1999	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley estatutaria 1581 de 2012,	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Norma técnica colombiana NTC ISO/IEC 27000	Tiene como objetivo definir requisitos para un sistema de gestión de la seguridad de la información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados y proporcionales, protegiendo así la información,
Norma técnica colombiana NTC - ISO/IEC 27001	ISO 27001 es una norma internacional, la cual permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas de gestión para su procesamiento. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.
Modelo Integrado de Planeación y Gestión	En su versión actualizada mediante el Decreto 1499 de 2017 emitido por el Departamento Administrativo de la Función Pública, es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión Institucional del MEN y sus Entidades Adscritas y Vinculadas, en términos de calidad e integridad del servicio, con el fin de la entrega de resultados para atender y resolver las necesidades y problemas de los grupos de valor.

Fuente: Construcción propia, investigación páginas web.

4 Plan de Seguridad de la Información (PSI).

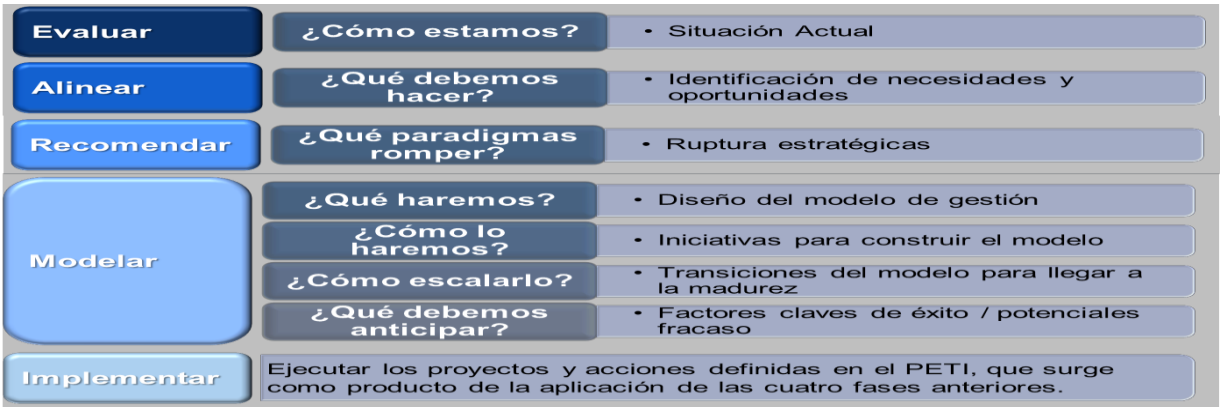
El Plan de Seguridad de la Información (PSI), es un documento cuyo objetivo trazar y planificar la manera como la entidad realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Este se indicará en plazos anuales, en los cuáles se harán las labores con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la Institución.

5 Metodología

Para la implementación del Modelo Integrado de Gestión de TI, teniendo como referente IT4+®, se estableció una metodología; la cual comprende actividades para cada uno de los componentes del modelo, así como las herramientas de apoyo a su aplicación. La primera actividad es la de Evaluar, hecha a nivel de Gobierno de TI, de Estrategia de TI, de Gestión de Información, de Sistemas de Información, de Servicios tecnológicos, de Uso y apropiación e Integralmente.

Tabla 3. Metodología de implantación del modelo IT4+®



Fuente: Tomado de Documento - versión actualizada del modelo de gestión IT4+®, MinTIC 2016

En el Anexo B, se relacionan las principales herramientas para ser aplicadas durante las fases de implementación del modelo. Algunas de ellas corresponden con entregables de la implementación del modelo, a saber: Caracterización de Sistemas de Información, Formatos de entrevistas, Formatos del Plan Estratégico de TI, Formatos del portafolio de proyectos, Presentación de gestión de información y la Matriz de artefactos. En otras palabras, estas herramientas se aplican durante la implementación del modelo y una vez diligenciadas, se convierten en parte de los entregables a suministrar a la entidad donde se está aplicando.

En la siguiente tabla se indica la forma de aplicar las herramientas en cada una de las fases de la metodología de implantación del modelo IT4+®, así como su correspondiente ubicación e identificación de archivo dentro del repositorio existente.

Tabla 4. Aplicación de las herramientas en la metodología

N°	Herramienta	Descripción general	Proceso cadena de valor asociado	Etapa metodología
1	Diagnóstico de la estrategia	Analizar el estado actual del planteamiento estratégico de la gestión de TI	Planear y dar lineamientos de TI	Diagnóstico
2	Rupturas estratégicas	Para cada momento en el camino de madurez, definir las acciones y rupturas estratégicas a seguir	Planear y dar lineamientos de TI	Diagnóstico
3	Modelo de madurez de gestión de TI	Ubicar la entidad1sector en el nivel de madurez definido por el modelo.	Planear y dar lineamientos de TI	Diagnóstico
4	Plan Maestro de TI	Mostrar la iniciativas a un nivel estratégico y ejecutivo	Planear y dar lineamientos de TI	Modelo de planeación
5	Transformación es clave del sector	Mostrar las acciones de transformación del sector	Planear y dar lineamientos de TI	Modelo de planeación

6	Alineación de objetivos	Cómo TI apoya los objetivos estratégicos	Planear y dar lineamientos de TI	Modelo de planeación
7	Portafolio de proyectos	Proyectos estratégicos y proyectos tácticos priorizados y caracterizados	Planear y dar lineamientos de TI	Modelo de planeación
8	Plan de inversión	Definir actividades estratégicas incluyendo costos por cada componente del modelo IT4+	Planear y dar lineamientos de TI	Modelo de planeación
9	Gestión Financiera (ejecución)	Seguimiento a la ejecución de los recursos financieros	Planear y dar lineamientos de TI	1mplementación del modelo
1O	Tablero de 1ndicadores de Seguimiento y Evaluación	Constar con un tablero para medir las principales indicadores de los proyectos estratégicos	Planear y dar lineamientos de TI	1mplementación del modelo

Fuente: Tomado de Documento - versión actualizada del modelo de gestión IT4+®, MinTIC 2016

6 Lineamientos para la elaboración del PSI.

El Plan de Seguridad de la Información (PSI), deberá indicar: plazos anuales, cuáles serán las labores a realizar por parte la Institución con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la entidad y debería contener como mínimo lo siguiente:

Tabla 5. Proceso y labores

Proceso	Labores
Requisitos generales	Preceptos básicos, deben cumplirse en el diseño SGSI
Establecimiento y gestión del MSPI	Establecimiento del MSPI
	Implementación y operación del MSPI
	Seguimiento y revisión del MSPI
	Mantenimiento y mejora del MSPI
Requisitos de documentación	Generalidades
	Control de Documentos
	Control de Registros
Responsabilidad de la Dirección de la Institución	Compromiso de la Dirección
	Gestión de Recursos
	Provisión de Recursos
	Formación, toma de conciencia y competencia
Auditorías internas del MSPI,	Actividad independiente y objetiva de aseguramiento y consultoría diseñada para agregar valor y mejorar las operaciones de una organización
Revisión del MSPI por la Dirección de la Institución	Generalidades
	Información para la revisión
	Resultados de la revisión
Mejora del MSPI	Mejora continua
	Acción correctiva
	Acción preventiva

Compatibilidad del MSPI con los otros Sistemas de Gestión	Alineamiento con otros sistemas de gestión

Fuente: Constricción propia, Información tomada del documento, Anexo 1 del Modelo de Seguridad y Privacidad de la Información Versión 4.0, MINTIC, febrero 2021- Lineamientos GD – MinTIC.

6.1 Requisitos generales.

La institución, impulsarán la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), en el contexto de las actividades globales y de los riesgos a enfrentar.

Para llevar a cabo este propósito, se basará en el modelo Planificar, Hacer, Verificar, Actuar (PHVA).

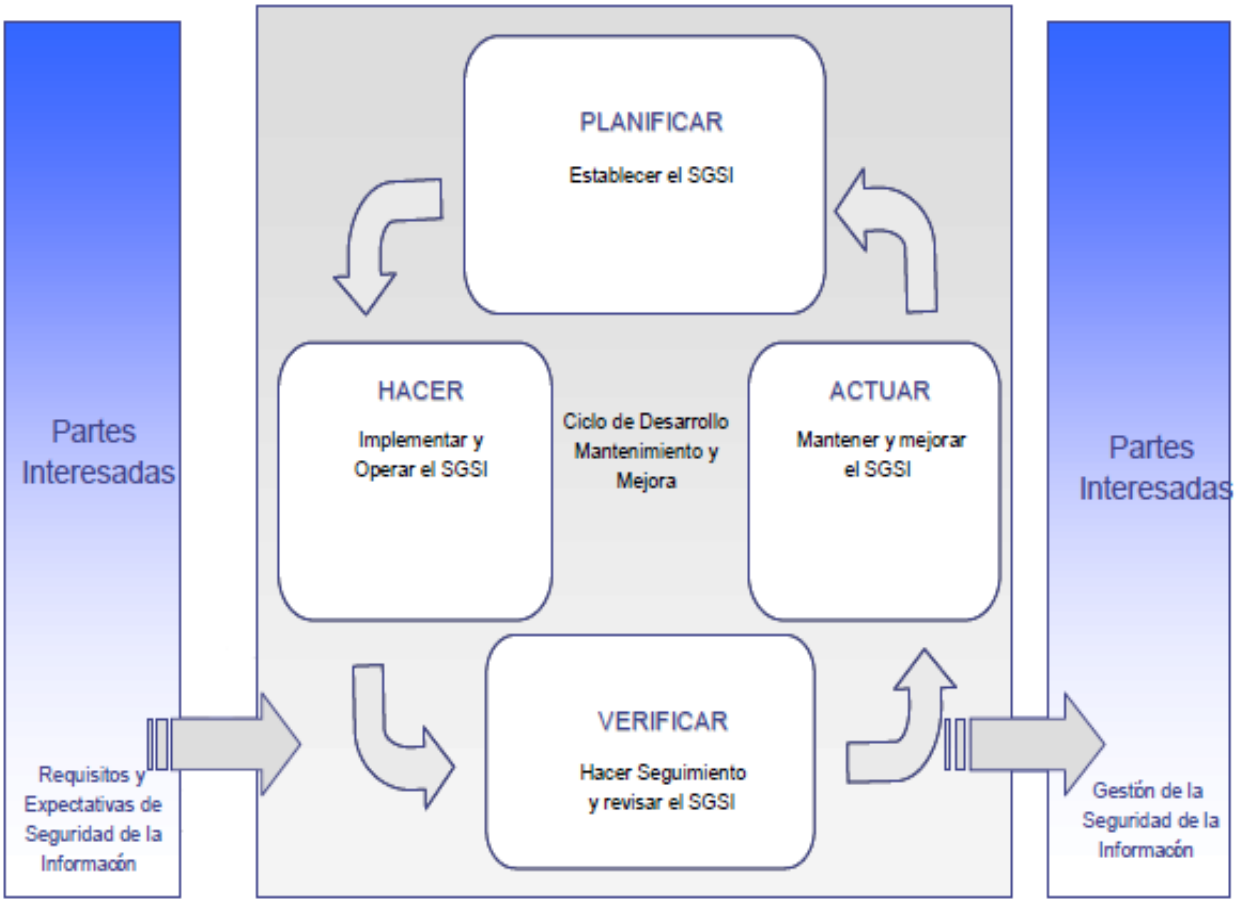


Ilustración 2. Modelo PHVA aplicado al MSPI
Fuente: Tomado del documento, Anexo 1 del Modelo de Seguridad y Privacidad de la Información Versión 4.0, MINTIC, febrero 2021- Lineamientos GD – MinTIC.

6.2 Ciclo operación.

El MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de los sujetos obligados un sistema de Gestión de Seguridad de la Información (SGSI) y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten a las Entidades gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, los sujetos obligados deben abordar las fases, las cuales están contempladas en el Anexo 1 del Modelo de Seguridad y Privacidad de la Información Versión 4.0, MINTIC, febrero 2021, Pág. 6-8.

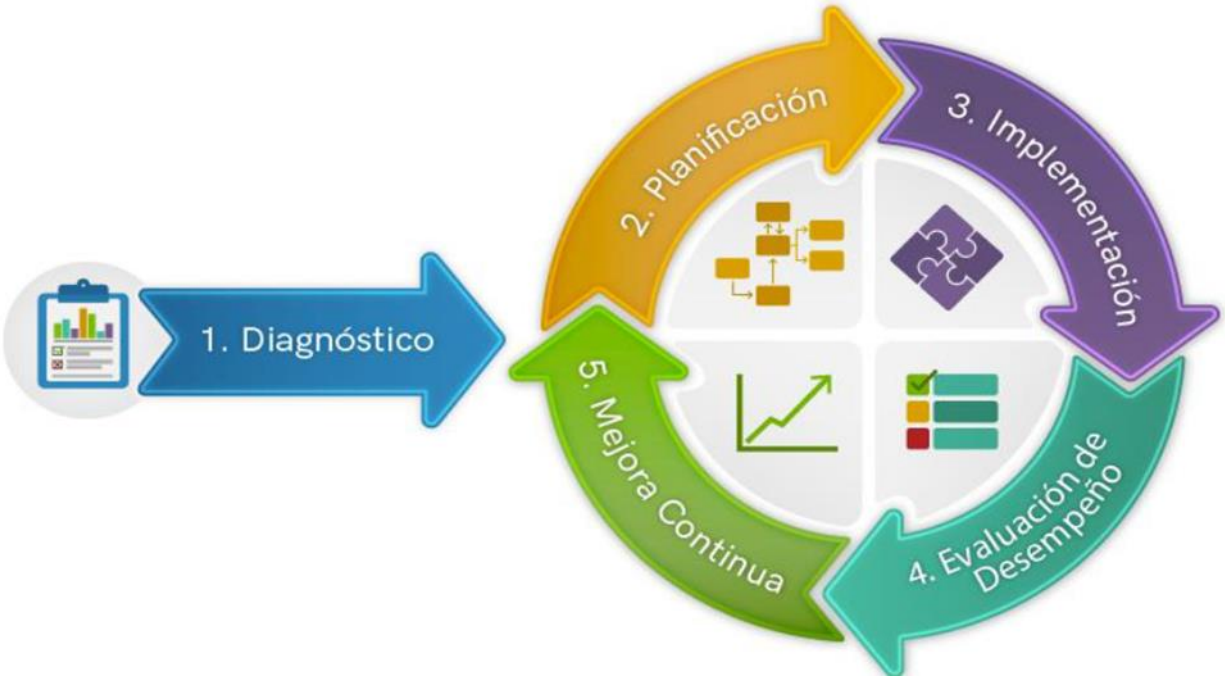


Ilustración 3. Metodología MSPI

El modelo de seguridad de la información del ITA, se estableció teniendo en cuenta las cinco (5) fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información como habilitadoras de la política de Gobierno Digital del Gobierno Nacional.

Tabla 6. Faces de Implementación

Fase y Objetivos	Acción	Actividad	Componente	Alineación NORMA ISO 27001:2013

DIAGNÓSTICO Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad de la Información.	Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, cuyo resultado sea un insumo para la fase de planificación y luego al finalizar la Fase de mejora continua.	Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.	Estado actual de la institución Identificación del nivel de madurez Levantamiento de información	En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del modelo de seguridad de la información.
PLANEACIÓN (PLANIFICAR, establecer el MSPI) En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.	Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más	A partir del diagnóstico, se definen las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo. Se definen, para todos los procesos institucionales, los límites de la implementación basados en el alcance.	Contexto de la institución • Entender la institución • Necesidades y expectativas de las partes interesadas • Determinar alcance del MSPI Liderazgo • Liderazgo y compromiso de la Dirección de la Institución. • Política de seguridad • Roles de la institución, responsabilidades y autoridad Planeación	En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Dirección de la Institución respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de establecer una política de seguridad de la información adecuada al propósito de la organización asegure la

	importante del ciclo. Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización		• Acciones para abordar los riesgos y oportunidades • Objetivos y planes para lograrlos Soporte • Recursos • Competencias • Sensibilización • Comunicación • Documentación	asignación de los recursos para la seguridad de la información y las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen. En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento. En el capítulo 7 – Soporte donde se establece: la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del modelo de seguridad de la Información
IMPLEMENTACIÓN (HACER, implementar y operar el MSPI) En esta fase se ejecuta el plan establecido el cual consiste en implementar las acciones para	Implementar los controles permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la	La ejecución de esta etapa permitirá a la Institución la implementación de los aspectos identificados en las fases anteriores	Control y planeación operacional Plan de Tratamiento de riesgos de seguridad y privacidad de la información	En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica a la organización planificar, implementar y controlar los procesos

lograr mejoras planteadas	información identificados en la etapa de planificación. (Implementar y operar la política, los controles, procesos y procedimientos del MSPI)	(diagnóstico y planeación)	Definición de Indicadores de Gestión	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.
EVALUACIÓN Y DESEMPEÑO (VERIFICAR hacer seguimiento y revisar el MSPI) Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.	Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición. Determinar el sistema y forma de evaluación de la adopción del modelo. Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la Dirección de la Institución, para su revisión	La evaluación se realiza en términos de efectividad, la eficiencia y la eficacia de las acciones implementadas, con base en los resultados de los indicadores definidos	Monitoreo, medición, análisis y evaluación Auditoría interna Revisión por la Dirección de la Institución.	En el capítulo 9 – Evaluación del desempeño, se 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.
MEJORA CONTINUA, (ACTUAR,	Emprender acciones correctivas y preventivas	La mejora continua se logra a través de la	Acciones correctivas	En el capítulo 10 - Mejora, se establece para el proceso de mejora

mantener y mejorar el MSPI) Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.	con base en los resultados de la auditoría interna del MSPI y la revisión por la Dirección de la Institución, para lograr la mejora continua del MSPI.	consolidación de los resultados de la evaluación, diseñando un plan de mejoramiento para mitigar las debilidades identificadas. Al finalizar cada fase se debe realizar una reunión con la Dirección de la Institución de la Institución para presentar el informe del avance del proyecto, (resumen ejecutivo), y evaluar posibles ajustes al mismo.	Oportunidades de mejora	del modelo de seguridad de la Información, donde a partir de las no conformidades ocurridas, 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 no repetición.

Fuente: Constricción propia, Información tomada del documento, Anexo 1 del Modelo de Seguridad y Privacidad de la Información Versión 4.0, MINTIC, febrero 2021- Lineamientos GD – MinTIC.

6.3 Descripción del ciclo de operación.

Este plan se implementará usando la metodología PHVA propuesta por MinTIC en el Modelo de Seguridad y Privacidad de la Información. En cada fase se ejecutarán las acciones y se elaborarán los documentos propuestos por MinTIC en el mismo modelo, acorde con los lineamientos de Modelo Integrado de Planeación y Gestión (MIPG).- Decreto 1499 de 2017 emitido por el Departamento Administrativo de la Función Pública.

Con base en los proyectos propuestos y ruta crítica para la ejecución de estos, se planifica la ejecución de los mismos con una proyección a cuatro años, para tal fin, se debe diligencia el Anexo C, Cronograma actividades PSI.

7 Comité de seguridad de la información

El Comité de Seguridad de la Información, fue creado en la Institución mediante acto administrativo como órgano responsable de la implementación, aplicabilidad y funcionalidad de la Política de Seguridad de la Información,

Política de Protección de Datos Personales y del Plan de Contingencia y Continuidad Informático, y el cual tiene dentro de sus funciones:

- Adoptar las medidas y acciones de conformidad con los resultados de los diagnósticos del estado de la seguridad de la información, con el fin de tomar y establecer las medidas necesarias.
- Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
- Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la Institución.
- Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
    - Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.
    - Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la Institución.
    - Aprobar acciones y mejores prácticas en la implementación del MSPI.
    - Adoptar las decisiones, permitiendo la gestión y minimización de riesgos críticos de seguridad de la información.
- Coordinar y dirigir acciones específicas en pro de proveer un ambiente seguro y establecer los recursos de información consistentes con las metas y objetivos la Institución.
- Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual, pérdidas patrimoniales o afectar los recursos de información de la Institución.
- Garantizar, hacer seguimiento y/o verificación de la implementación del Modelo de Seguridad y Privacidad (MSPI) de la Información al interior de la Institución.
- Garantizar, hacer seguimiento y/o verificación de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Institución.
- Participar en la formulación y evaluaciones los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- Poner en conocimiento de la Institución, los documentos generados al interior del Comité de Seguridad de la Información, cuyo accionar impacten de manera transversal a la misma.

- Promover la difusión y sensibilización de la seguridad de la información dentro de la Institución.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de la Institución.
- Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SCSI de la Institución.
- Realizar revisiones periódicas del Sistema de Gestión de Seguridad de la Información (SGSI) (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- Recomendar roles y responsabilidades específicos, relacionados con la seguridad de la información.
- Revisar, acompañar, impulsar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
- Supervisar la integración del Sistema de Gestión de Seguridad de la Información (SGSI) con los demás Sistemas de Gestión de la Institución.
- Las demás funciones inherentes a la naturaleza del Comité, relacionadas con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

Funciones de la Secretaría Técnica

- Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
- Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
- Llevar la custodia y archivo de las actas y demás documentos soportes.
- Presentar los informes requeridos por el Comité.
- Realizar seguimiento a los compromisos y tareas pendientes del Comité.
- Recibir y preparar la respuesta a los documentos, competentes con el Comité.
- Remitir oportunamente a los miembros la agenda de cada comité.
- Servir de interlocutor entre terceros y el Comité.
- Verificar el quórum al inicio de las sesiones
- Firmar las actas aprobadas por el Comité.

Las funciones de este Comité pueden ser incluidas por el **Comité Institucional de Desarrollo Administrativo**, como instancia orientadora de la implementación de la estrategia de Gobierno en línea de acuerdo con el señalado en el Decreto 1078 de 2015, Artículo 2.2.9.1.2.4. Responsable de orientar la implementación de la Estrategia de Gobierno en línea. En las entidades del orden nacional, el **Comité Institucional de Desarrollo Administrativo**, artículo 6 del Decreto 2482 de 2012, o

las normas que lo modifiquen o sustituyan, será la instancia orientadora de la implementación de la Estrategia de Gobierno en línea al interior de cada entidad. Los sujetos obligados deberán incluir la estrategia de Gobierno en línea de forma transversal dentro de sus planes estratégicos sectoriales e institucionales, y anualmente dentro de los planes de acción de acuerdo con el Modelo Integrado de Planeación y Gestión, Decreto 2482 de 2012. En estos documentos se deben definir las actividades, responsables, metas y recursos presupuesta para dar cumplimiento a los lineamientos establecidos.

En el Anexo A, se presenta un ejemplo de plantilla, la cual podría servir como base para la generación de la resolución para la creación del Comité de Seguridad de la Información para las Institución, (está sujeta a las condiciones orgánicas y misionales institucionales).

8 Equipo de respuesta incidentes de seguridad de la información

Este equipo hace parte del Modelo de Gestión de Incidentes de Seguridad de la Información (GISI), cuyo objetivo principal es tener un enfoque estructurado y bien planificado, por lo cual, permita manejar adecuadamente los incidentes de seguridad de la información, donde, los objetivos del modelo son garantizar que:

- Definir roles y responsabilidades dentro de la Organización como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio.
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
- Minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.
- Consolidar los incidentes de seguridad de la información de las lecciones aprendidas y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.
- Definir los mecanismos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.

- Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
- Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información.

Para lograr estos objetivos, la gestión de incidentes de seguridad de la información involucra los siguientes procesos de manera cíclica como lo muestra la imagen:

- Planificación y preparación para la gestión del Incidente
- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividades Post-Incidente.

El documento Guía 21 - Gestión de Incidentes, permite a las entidades estar preparadas para afrontar cada una de las etapas anteriores, y adicionalmente definiendo responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

La Guía 21 - Gestión de Incidentes, plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad. La cual incorporó los componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013 para la estrategia de Gobierno en Línea.

Es recomendable por partes de las entidades creen un Equipo de respuesta incidentes de seguridad de la información (CSIRT) o un grupo que se haga responsable, quienes se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargaran de:

- **Detección de Incidentes de Seguridad:** Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.

- **Atención de Incidentes de Seguridad**: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- **Recolección y Análisis de Evidencia Digital:** Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- **Anuncios de Seguridad:** Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
- **Auditoria y trazabilidad de Seguridad Informática:** El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- **Certificación de productos:** El equipo verifica la implementación de las nuevas aplicaciones en producción ajustadas a los requerimientos de seguridad informática definidos por el equipo.
- **Configuración y Administración de Dispositivos de Seguridad Informática:** Se encargaran de la administración adecuada de los elementos de seguridad informática.
- **Clasificación y priorización de servicios expuestos:** Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- **Investigación y Desarrollo:** Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Este grupo está enfocado principalmente en atender los incidentes de seguridad de la información presentados sobre los activos soportados por la plataforma tecnológica de la entidad, quién tendrá a su cargo las siguientes funciones:

- Emitir concepto sobre los aspectos necesarios para garantizar la seguridad de la Información.
- Proponer los temas, la información y los indicadores determinados por el Comité de Seguridad de la Información, considerados de interés de la Entidad.
- Asesorar y proponer acciones para orientar y mejorar la Seguridad de la Información de la
- Presidencia de la República.
- Coordinar con el Área de Tecnologías de la Información y Sistemas, la definición de proyectos y medidas de seguridad de la Información.
- Realizar el registro detallado e informar oportunamente la ocurrencia de eventos e incidentes de seguridad de la información, con el fin de tomar

las acciones correspondientes al área de Tecnologías y Sistemas de información.

- Establecer contacto con diferentes organismos especializados en materia de seguridad de la información, de acuerdo al marco de cooperación nacional definido en el CONPES 3854 de 2016.

9 Equipo de proyectos.

Se debe conformar un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar la disponibilidad oportuna de la información relevante de la entidad. De esta forma se busca asegurar una iniciativa de carácter transversal a la entidad, y al no depender exclusivamente de la oficina o área de TI. Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

Ilustración 4. Equipo de Gestión de Seguridad de la Información.
Fuente: Tomado de Documento, *Guía 4 - Roles y responsabilidades* . 2016 - MinTIC.

Dentro de las responsabilidades del equipo del proyecto, se tiene:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento, suscitadas en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.

- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.

De manera particular se resaltan dos perfiles participantes de manera activa durante el desarrollo del proyecto, (el proyecto no es de responsabilidad exclusiva del área de TI), donde, su papel es fundamental, y de acuerdo a la Ley de Protección de Datos Personales se debe tener muy presente el rol de Responsable del tratamiento de los datos personales.

Teniendo en cuenta, el responsable del tratamiento de datos personales en la entidad, es quien tiene decisión sobre las bases de datos y es el responsable de direccionar las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales obtenidos mediante autorización, en el caso de ser requerido.
- Respetar las condiciones de seguridad y privacidad de información del titular.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

En la siguiente Ilustración están representados los conceptos del Modelo de Gestión de Proyectos (MGPTI). Los principios establecen directrices para realizar un proceso efectivo de gestión de proyectos, éstos a su vez son la base en la estructuración de los dominios; los dominios agrupan lineamientos, los cuales son implementados a través de las diferentes guías creadas por el MinTIC.

El proceso de gestión de proyectos está compuesto por fases desglosadas en actividades, las cuales son los elementos mínimos y fundamentales del modelo. En la aplicación de las guías y actividades se producen evidencias o entregables, en conjunto constituyen el repositorio de la oficina o dependencia encargada del portafolio de proyectos.

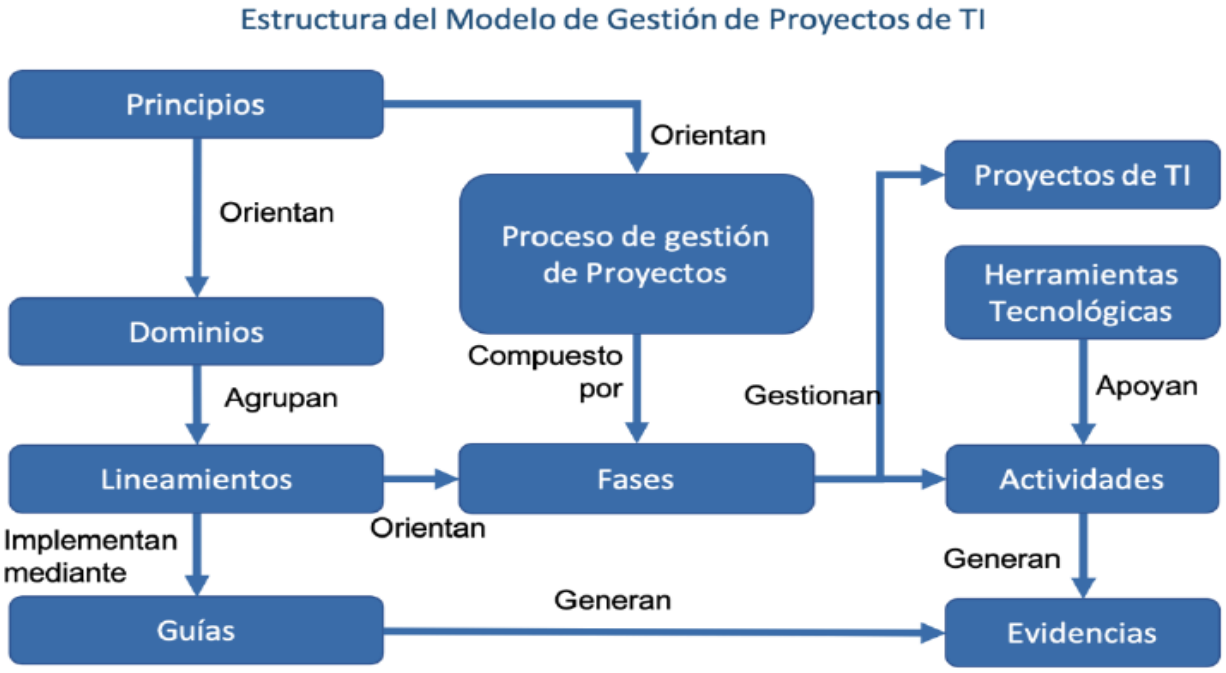


Ilustración 5. Estructura del Modelo de Gestión y Gobierno de TI.
Fuente: Tomado de Documento, MGPTI.G.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI. 2019 MinTIC.

9.1 Planeación, ejecución y seguimiento

La gestión de proyectos de TI debe realizarse teniendo en cuenta cinco procesos: Inicio, Planeación, Ejecución, Control y Cierre. En todos los proyectos y en cada uno de estos procesos deben tenerse en cuenta las siguientes dimensiones, las cuales deben ser estructuradas y gerenciadas de manera integral: Alcance, Costos, Tiempo, Equipo Humano, Compras, Calidad, Comunicación, Manejo de Personas interesadas (Stakeholders) e Integración. Adicionalmente a los conocimientos básicos de gerencia de proyectos, éstos se deben complementar con: Conocimientos y habilidades gerenciales, conocimientos en normas y regulaciones del área de aplicación, habilidades interpersonales, comprensión del entorno del proyecto, orientación al logro, entre otras competencias.

9.2 Control de cambios

Una vez establecido el alcance inicial y teniendo en cuenta las condiciones de calidad, de tiempo, costos y recursos; los cambios surgidos, deben evaluarse a

la luz de las implicaciones en cada una de las dimensiones mencionadas. De ser necesario realizar un cambio en el proyecto afectado por la calidad de los entregables, el tiempo de ejecución, los costos financieros o los recursos involucrados, el cambio debe revisarse y deberá documentarse y acordarse entre las partes y se formalice en la documentación de los proyectos y, si aplica, en las condiciones contractuales.

9.3 Indicadores de gestión de los proyectos

Para establecer el avance y la ejecución normal de los proyectos se debe contar con un conjunto de indicadores, los cuales permitan registrar y monitorear el estado del proyecto.

Se deben definir pocos indicadores para medir el avance de los entregables, el gasto causado, el valor ganado y los resultados obtenidos.

De esta manera si adelantará el proceso de control para medir la eficiencia, la eficacia y la efectividad del proyecto. Estos se utilizarán para medir la gestión de los procesos de TI, como se muestra en el Anexo D.

Anexo A. Herramientas de la metodología.

En este anexo encontrará la información relacionada con las herramientas de la metodología y los mecanismos de acceso a las mismas. A continuación se muestra la especificación de las herramientas indicando su descripción, nombre del archivo de guía descriptiva para su apropiación y uso, nombre del archivo de la herramienta y para cada herramienta se indica la(s) hoja(s) del libro de Excel con los formatos a aplicar para cada herramienta.

Las guías de uso y los archivos de las herramientas se encuentran en la carpeta Herramientas del repositorio del modelo. Además, a cada guía y herramienta se le asoció un hipervínculo para utilizarlo durante la navegación de este documento.

Tabla 7. Herramientas en la metodología de implantación.

N°	Herramienta	Descripción general	Guía de uso	Archivo herramienta	Hojas de la herramienta
1	Diagnóstico de la estrategia	Analizar el estado actual del planteamiento estratégico de la gestión de TI	IT4+_F1CHATOL_01_Entrevista Estrategia.pdf	IT4+_TOOL_01_Entrevista Estrategia.xlsx	Formato
2	Rupturas estratégicas	Para cada momento en el camino de madurez, definir las acciones y rupturas estratégicas a seguir	IT4+_F1CHATOL_02_Rupturas Estrategicas.pdf	IT4+_TOOL_02_rupturas Estrategicas.xlsx	Estrategia TI, Gobierno TI, Información, Sistemas, ServiciosTec, Uso, Madurez
3	Modelo de madurez de gestión de TI	Ubicar la entidad1sector en el nivel de madurez definido por el modelo.	IT4+_F1CHATOL_03_Madurez de la Gestión CON TI.pdf	IT4+_TOOL_03_Madurez de la Gestión CON TI.xlsx	Encuesta, Madurez, Niveles de Madurez
4	Plan Maestro de TI	Mostrar la iniciativas a un nivel estratégico y ejecutivo	IT4+-F1CHATO OL-06-Plan Maestro TI.pdf	IT4+-TOOL-04-05-06-AL1NEAC1ÓN-TRANSFORMAC1ÓN-PLANMAESTRO.xlsx	4.Plan Maestro TI
5	Transformaciones clave del sector	Mostrar las acciones de transformación del sector	IT4+-F1CHATO OL-05-Transformaciones de Negocio.pdf	IT4+-TOOL-04-05-06-AL1NEAC1ÓN-TRANSFORMAC1ÓN-PLANMAESTRO.xlsx	2.Transformaciones con TI 3.Capacidades TI

			IT4+-F1CHATO OL-05A-Capaci dadas Requeridas.pdf		
6	Alineación de objetivos	Cómo TI apoya los objetivos estratégicos	IT4+-F1CHATO OL-04-Objetivo s Estratégicos.pdf	IT4+-TOOL-04-05-06-AL1NEAC1ÓN-TRANSF ORMAC1ÓN-PLANMAEST RO.xlsx	Datos Sector 1.Objetivos Estratégicos
7	Portafolio de proyectos	Permite realizar el seguimiento gerencial periódico de los avances de los proyectos y logro de los objetivos de la Estrategia de TI.	IT4+-F1CHATO OL-08-Portafoli o de proyectos.pdf	IT4+-TOOL-07-08-09-10--PROYECTOS-PLAN1NVERS1ON-SEGF1NANC1ERO-1ND1CADORE S.xlsx	• PE-Variación presupuesto • PE-Definición Proyectos Estratégicos • PE-Indicadores • PT-Estado Portafolio • PT-Portafolio • PT-Avance proyectos
8	Plan de inversió n	Definir actividades estratégicas incluyendo costos por cada componente del modelo IT4+®	IT4+-F1CHATO OL-07-Plan de inversión.pdf	IT4+-TOOL-07-08-09-10--PROYECTOS-PLAN1NVERS1ON-SEGF1NANC1ERO-1ND1CADORE S.xlsx	- PC-Seguimiento plan de compras - PC-Plan de compras
9	Gestión Financiera (ejecució n)	Seguimiento a la ejecución de los recursos financieros	IT4+-F1CHATO OL-09-Seguimi ento ejecución financiera.pdf	IT4+-TOOL-07-08-09-10--PROYECTOS-PLAN1NVERS1ON-SEGF1NANC1ERO-1ND1CADORE S.xlsx	- PC-Ejecución financiera
10	Tablero de Indicadores de Seguimiento y Evaluación	Constar con un tablero mida las principales indicadores de los proyectos estratégicos	IT4+-F1CHATO OL-10-1ndicado res.pdf	IT4+-TOOL-07-08-09-10--PROYECTOS-PLAN1NVERS1ON-SEGF1NANC1ERO-1ND1CADORE S.xlsx	- PE-Indicadores

Fuente: Tomado de Documento - versión actualizada del modelo de gestión IT4+®, MinTIC 2016

Anexo B. Cronograma de actividades PSI.

Tabla 8, Cronograma actividades PSI.

Fase	Actividades	Entregable	Fecha	% Ejecución
DIAGNÓSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información	Diligenciar la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la Entidad, y sus acciones de mejora. Con vigencia.		
	Identificar el nivel de madurez de seguridad y privacidad de la información en la Institución	Diligenciar la herramienta de identificación de madurez.		
	Identificar vulnerabilidades técnicas y administrativas, las cuales sirven como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad		
PLANEACIÓN (PLANIFICAR, establecer el MSPI)	Revisar las Política de Seguridad y Privacidad de la Información	Elaborar actualización Política de seguridad y privacidad de la información, enviar a jurídica la memoria justificativa y a las partes interesadas el documento para aprobación.		
		Manual con las políticas de seguridad y privacidad de la información aprobadas y socializadas		
	Procedimientos de seguridad de la información (Plan de Calidad)	Actualizar Procedimientos (planes de calidad), debidamente documentados, socializados y aprobados por el		

		comité de Sistemas de Gestión Institucional.		
	Roles y responsabilidades de seguridad y privacidad de la información.	Definir y aprobar Roles y responsabilidades mediante Resolución Rectoral a través del cual se definen las instancias al interior de la institución, las cuales se encargarán de revisar, de velar el Cumplimiento y el mejoramiento continuo de la política de Seguridad y privacidad de la información de la unidad central del valle del cauca, revisada y aprobada por la Dirección de la Institución.		
	Identificación, documentación y aprobación del Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado, revisado y aprobado		
		Matriz con la identificación, valoración y clasificación de activos de información.		
		Documento con la caracterización de activos de información, contenedores de datos personales		
		Inventario de activos de IPv6		
	Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.		
	Plan de Tratamiento de Riesgos de	Elaborar y presentar para aprobación del Plan de Tratamiento de		

	Seguridad y Privacidad de la Información.	Riesgos de Seguridad Digital		
		Actualizar Riesgos mediante documento Matriz con la metodología de gestión de riesgos, análisis y evaluación de riesgos.		
		Documento con la declaración de aplicabilidad.		
		Documentos revisados y aprobados por la Dirección de la Institución.		
	Plan de capacitación, sensibilización y comunicación de seguridad de la información.	Diseñar y aprobar programas y planes para los funcionarios sobre conciencia y comunicación de las políticas		
		Documento con el plan de comunicación, sensibilización y capacitación para la entidad.		
	Implementar el Modelo de Seguridad y Privacidad de la Información	Documento del análisis de lo alcanzado en Madurez Inicial		
	Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.		
IMPLEMENTACIÓN (HACER, implementar y operar el MSPI)	Plan de Implementación de controles de seguridad	Elaborar el Plan de Implementación de controles de seguridad digital		
	Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado.		
	Implementación del plan de	Verificar inicialmente ejecución de acciones para el tratamiento de		

	tratamiento de riesgos.	riesgos, mediante un informe de la ejecución del plan de tratamiento de riesgos aprobado por el responsable de cada proceso.		
	Indicadores de Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.		
	Evidencia de los controles implementados y las mejoras presentadas anualmente	Diligenciar y actualizar Matriz de evaluación de Controles ISO 27001-2013 con las Evidencias de la implementación de los controles de seguridad Digital		
	Plan y estrategia de transición de IPv4 a IPv6.	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina Gestión de TI.		
	Implementación del Plan y estrategia de transición de IPv4 a IPv6.	Implementar el plan		
	Plan de pruebas de funcionalidad de IPv4 a IPv6	Implementar el plan		
EVALUACIÓN Y DESEMPEÑO (VERIFICAR hacer seguimiento y revisar el MSPI)	Indicadores de seguridad Digital	Actualizar la Tabla de Indicadores Seguridad Digital y enviar a responsable de plan de acción		
	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 Dirección de la Institución.		
	Ejecución y evaluación del Plan Tratamiento de Riesgos de Seguridad Digital	Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en		

		el plan de tratamiento de riesgos		
	Gestión de Incidentes de Seguridad de la Información	Elaborar y enviar el informe de gestión de incidentes de seguridad de la vigencia		
	Evaluación de Plan de Continuidad de la Operación de los Servicios TI de la Institución	Realizar Informe de cumplimiento del Plan de Continuidad de la Operación de los Servicios		
	Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Dirección de la Institución.		
		Solicitar la programación de autoría del MSPI, la cual será incluida en el Plan de Auditorías		
	Evaluación del plan de seguridad	Realizar presentación de cumplimiento del plan de seguridad y privacidad de la Información y enviar para ser presentado para aprobación		
	Autodiagnóstico nivel de madurez	Realizar Autodiagnóstico		
	Identificación del nivel madurez	Realizar Autodiagnóstico		
	Análisis de brecha	Realizar Análisis		
MEJORA CONTINUA (ACTUAR, mantener y mejorar el MSPI)	Plan de mejora continua	Elaborar documento con el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.		

		Documento con el plan de comunicación de resultados.		
	Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI	Socializar resultados del plan		
	Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.	Socializar resultados del plan		
	Contar con una herramienta de análisis sobre impacto en la privacidad	Realizar la herramienta de análisis sobre impacto en la privacidad		
	Descripción de los flujos de información	Documentar procesos		
	Identificar los riesgos de privacidad	Elaborar matriz de riesgos de privacidad		
	Cumplimiento plan de mejora	Evaluación de planes de mejora		

Fuente: Construcción propia

Anexo C. Planilla resolución Comité de Seguridad de la Información

RESOLUCIÓN XX DE XXXX

"Por la cual se conforma el Comité de Seguridad de la Información del Instituto Técnico Agrícola (ITA) y se definen sus funciones"

EL RECTOR DE LA INSTITUCIÓN DE EDUCACIÓN SUPERIOR ITA, en uso de sus facultades legales y en especial las que le confiere el Estatuto General y la Resolución 0652 de 2012 del Ministerio del Trabajo, y,

CONSIDERANDO

Que….

…Que, en mérito de lo expuesto,

RESUELVE:

Artículo 1°. Conformación del Comité de Seguridad de la Información. Créase el Comité de Seguridad de la Información de del Instituto Técnico Agrícola (ITA). El Comité estará integrado así:

1. Representante del área de informática o su delegado.
2. Representante del área de Planeación o su representante.
3. Representante del área Jurídica (según corresponda por distribución Orgánica de la Institución) o su delegado.
4. Representante del área de Gestión de Calidad (según corresponda por distribución Orgánica de la Institución) o su delegado
5. Representante del área de Gestión Documental (según corresponda por distribución Orgánica de la Institución) o su delegado.
6. Representante del área de Control Interno o su delegado (según corresponda por distribución Orgánica de la Institución)
7. El responsable de Seguridad de la información de la Institución.

Parágrafo 1º.El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas consideradas necesarias por la naturaleza de los temas a tratar.

Artículo 2º. Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar la exista de una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Artículo 3°. Funciones del comité. El Comité de Seguridad de la Información del Instituto Técnico Agrícola (ITA) tendrá dentro de sus funciones las siguientes:

1. Adoptar las medidas y acciones de conformidad con los resultados de los diagnósticos del estado de la seguridad de la información, con el fin de tomar y establecer las medidas necesarias.
2. Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
3. Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
4. Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la Institución.
5. Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
    a. Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.
    b. Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la Institución.
    c. Aprobar acciones y mejores prácticas en la implementación del MSPI.
    d. Adoptar las decisiones, permitiendo la gestión y minimización de riesgos críticos de seguridad de la información.
6. Coordinar y dirigir acciones específicas en pro de proveer un ambiente seguro y establecer los recursos de información consistentes con las metas y objetivos la Institución.
7. Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual, pérdidas patrimoniales o afectar los recursos de información de la Institución.
8. Garantizar, hacer seguimiento y/o verificación de la implementación del Modelo de Seguridad y Privacidad (MSPI) de la Información al interior de la Institución.
9. Garantizar, hacer seguimiento y/o verificación de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Institución.
10. Participar en la formulación y evaluaciones los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
11. Poner en conocimiento de la Institución, los documentos generados al interior del Comité de Seguridad de la Información, cuyo accionar impacten de manera transversal a la misma.
12. Promover la difusión y sensibilización de la seguridad de la información dentro de la Institución.
13. Promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de la Institución.

14. Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SCSI de la Institución.
15. Realizar revisiones periódicas del Sistema de Gestión de Seguridad de la Información (SGSI) (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
16. Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
17. Recomendar roles y responsabilidades específicos, relacionados con la seguridad de la información.
18. Revisar, acompañar, impulsar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
19. Supervisar la integración del Sistema de Gestión de Seguridad de la Información (SGSI) con los demás Sistemas de Gestión de la Institución.
20. Las demás funciones inherentes a la naturaleza del Comité, relacionadas con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

Parágrafo 2. Una vez conformado el Comité de Seguridad de la Información, este podrá expedir su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señalas en el presente artículo.

Artículo 5°. Secretaria Técnica: La Secretaría Técnica del Comité se definirá al interior del Comité y el secretario elegido será remplazado cada XXXX (X) meses.

Artículo 6°. Funciones de la Secretaría Técnica. Las funciones de la Secretaría Técnica serán las siguientes:

1. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
2. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
3. Llevar la custodia y archivo de las actas y demás documentos soportes.
4. Presentar los informes requeridos por el Comité.
5. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
6. Recibir y preparar la respuesta a los documentos, competentes con el Comité.
7. Remitir oportunamente a los miembros la agenda de cada comité.
8. Servir de interlocutor entre terceros y el Comité.
9. Verificar el quórum al inicio de las sesiones
10. Firmar las actas aprobadas por el Comité.

Artículo 7°. Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse (según periodicidad definida por la Institución), previa convocatoria del Secretario Técnico del Comité.

Artículo 8°. Sesiones Extraordinarias. Los miembros del Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo con temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

Artículo 9°. Vigencia y Derogatoria: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dado en XXXX, a los X días del mes de XXXX de XXXX

Directivo Responsable de la Institución

Cargo

Fuente: Tomado de Documento, Guía 4 - Roles y responsabilidades *. 2016 - MinTIC.*

Anexo D. Indicadores de Gestión

En este anexo encontrará la información relacionada con los indicadores de gestión definidos por IT4+®. A continuación se muestra la especificación, indicando su nombre, descripción, nombre del archivo del indicador, además, a cada indicador se le asoció un hipervínculo para utilizarlo desde la navegación de este documento.

Tabla 9. Indicadores de gestión.

Nombre	Descripción	Archivo de la hoja de vida del indicador
Nivel de ejecución del Plan de Estratégico de TI	Medir en avance en la ejecución de los proyectos y actividades del plan estratégico de TI	Indicadores de Gestión IT4+.xlsx Hoja: Nivel ejecución PETI
Base de datos con aseguramiento	Uso efectivo de los sistemas y servicios de información de la entidad, en función de las bases de datos, cumplan los requisitos de conformidad, desarrollados a través de los procesos de gestión de TI.	Indicadores de Gestión IT4+.xlsx Hoja: BD con aseguramiento
Disponibilidad de información en medios de TI.	Uso efectivo de los sistemas y servicios de información de la entidad	Indicadores de Gestión IT4+.xlsx Hoja: Disp Info medios TI
Nivel de requerimientos de desarrollo y mantenimiento implementados	Medir el avance en el desarrollo de los requerimientos y el mantenimiento de los sistemas de información con respecto a las necesidades de la arquitectura institucional.	Indicadores de Gestión IT4+.xlsx Hoja: Requerimientos
Disponibilidad de las capacidades	Medir el nivel de operación para mantener el uso de los sistemas de información con base en la plataforma tecnológica	Indicadores de Gestión IT4+.xlsx Hoja: Interoperar
Oportunidad en la solución a novedades de la plataforma tecnológica	Medir la oportunidad en la solución de novedades para mantener el uso de los sistemas de información con base en la plataforma tecnológica	Indicadores de Gestión IT4+.xlsx Hoja: Oportunidad

Fuente: Tomado de Documento - versión actualizada del modelo de gestión IT4+®, MinTIC 2016