# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024

ESE CENTRO DE SALUD DE GALAPA

Contenido

## INTRODUCCION

La planificación e implementación del Plan de Seguridad y Privacidad de la Información – PSPI de la E.S.E. Centro de Salud de Galapa, está influenciado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad. De acuerdo a la necesidad de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos, la E.S.E. Centro de Salud de Galapa, adopta el Plan de Seguridad y Privacidad de la Información – PSPI del Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC, entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. A través del decreto 1078 de 2015, por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de Información y las Comunicaciones, en el TITULO 9, POLÍTICAS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN, CAPITULO 1, Estrategia de Gobierno en Línea - GEL, en la SECCIÓN 2, COMPONENTES, INSTRUMENTOS Y RESPONSABLES, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL, y es de obligatorio cumplimiento para las entidades del estado como lo establece en la sección 3, MEDICIÓN, MONITOREO Y PLAZOS. 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 Plan 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: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión y con el fin de facilitar la apropiación del modelo y su correcta implementación en las entidades, se recoge además de los cambios técnicos de la norma, herramientas específicas de privacidad relacionadas con las normas y los retos que el nuevo marco normativo (Ley de datos personales, Transparencia y Acceso a la Información Pública, entre otras), las cuales se deben tener en cuenta para la gestión de la información, así como los lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano. Finalmente, a nivel metodológico es importante tener presente que se han incluido una serie de guías en cada una de las fases del modelo, para que los destinatarios del mismo tengan claridad de cuáles son los resultados a obtener y como desarrollarlos.

## 1. JUSTIFICACIÓN

La E.S.E. Centro de Salud de Galapa, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un estado más eficiente, transparente y participativo, expone el Plan 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. Mediante el aprovechamiento de las TIC y el Plan de Seguridad y Privacidad de la Información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana. El Plan de Seguridad y Privacidad de la Información, es un documento vivo que permite actualizaciones con el fin de estar alineado con mejores prácticas, como la ISO 27001, Cobit, ITIL, Marco de Referencia de Arquitectura TI y recomendaciones hechas por organizaciones como el Convenio de Budapest y la Organización para la Cooperación y el Desarrollo Económico (OCDE), Organización de Estados Americanos - OEA, entre otros; donde las entidades del estado se vean beneficiadas con la construcción e implementación del mismo. Esto también permite llevar a las instituciones del estado a un mejor nivel de seguridad que refleje los avances del país en la materia, sirviendo de base para la identificación de las infraestructuras críticas y mejorar su respuesta ante las amenazas que afectan la Seguridad Digital.

## 2. GLOSARIO

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **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).
- **Ciber seguridad:** 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:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).

- **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.
- **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).
- **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).
- **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).
- **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).
- **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).
- **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

## 3. OBJETIVO

Presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de controles de seguridad según el modelo del Sistema de Gestión de Seguridad de la Información (MSPI), incorporando la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información la E.S.E. Centro de Salud de Galapa, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

## 4. OBJETIVOS ESPECIFICOS

- Comunicar e implementar la estrategia de seguridad de la información.
- Contribuir al incremento de la transparencia en la gestión pública.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Orientar a las entidades en las mejores prácticas para la construcción de una política de privacidad respetuosa de los datos personales de los titulares.
- Optimizar la gestión de la información al interior de las entidades destinatarias.

## 5. ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos de la ESE Centro de Salud de Galapa, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea (GEL) con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos para el Centro de Salud de Galapa.

## 6. MARCO LEGAL

| NORMA | DESCRIPCION |
|---|---|
| Decreto 1078 de 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. |
| NTC / ISO 27001:2013 | Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. |
| NTC/ISO 27002:2013 | Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. |

## 7. CONOCIMIENTO DE LA ENTIDAD

### 7.1 MISION

Prestar servicios de salud de baja complejidad, con énfasis en promoción de la salud, prevención de la enfermedad, diagnóstico y tratamiento integral de patologías que afecten la población de nuestra área de influencia, comprometidos a través de los convenios docentes –asistenciales a la formación integral de personas que propendan por alcanzar la excelencia, competentes en el área profesional y con responsabilidad social, basados en los principios de calidad, eficiencia, equidad y compromiso social, con un recurso humano capacitado y comprometido con el desarrollo, implementación y seguimiento de políticas que garanticen una atención segura, respeto por los deberes y derechos de todos de nuestros clientes internos y externos.

### 7.2 VISION

**En el 2025 la ESE HOSPITAL LOCAL DE GALAPA,** se posicionará como líder entre las instituciones prestadoras de servicios de salud de baja complejidad del departamento del Atlántico, prestando servicios con calidad, igualdad, oportunidad, constituyéndose en generadora de conocimiento y abanderada del restablecimiento de los derechos de nuestros usuarios y trabajando arduamente en la consolidación de una cultura de seguridad en la atención en salud.

### 7.3 ESTRUCTURA ORGANICA

La estructura organizacional de la ESE Centro de Salud de Galapa está definida en su creación mediante el Acuerdo 027 de 1996; Acto Administrativo de Adopción de Estatutos Resolución N° 013 de 1999, Resolución 0097 de 20202.


## 8. MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de operación, contempla un ciclo de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. En el presente Plan de Seguridad y Privacidad de la Información se contemplan diferentes niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación. La Seguridad y Privacidad de la Información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de 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, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad. 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, 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.

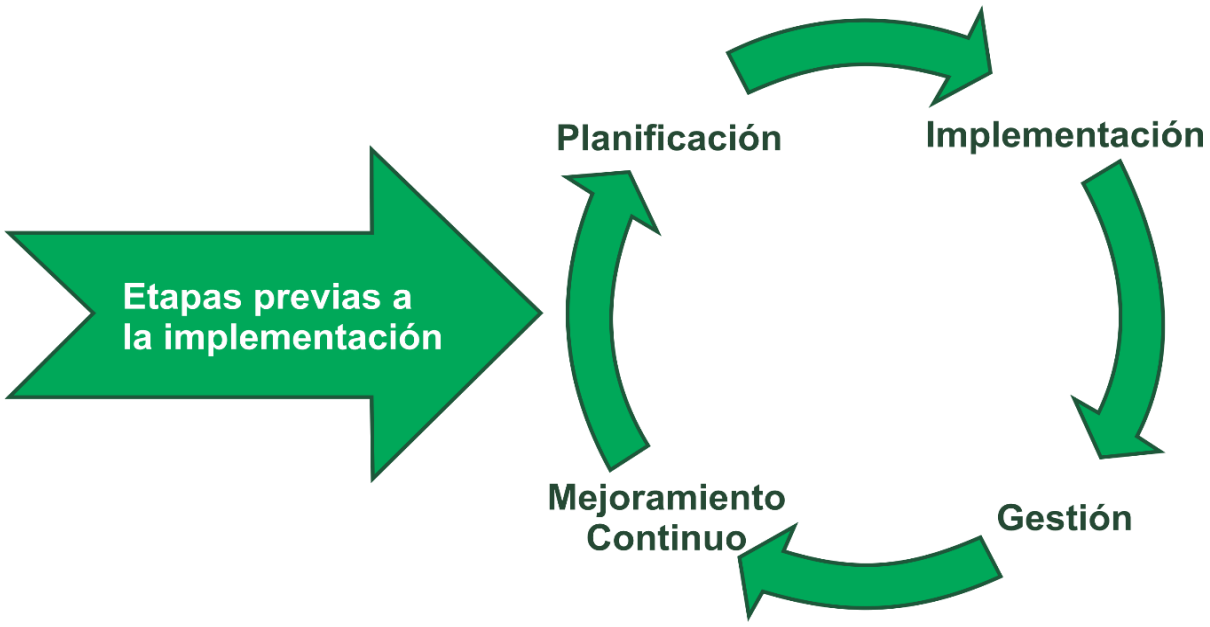
TIC para Gobierno Abierto y Seguridad y Privacidad de la Información se alinean en la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información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

sean confiables. Para lograr que los sistemas de información de la administración pública estén conectados, articulados, cumplan estándares y adopten las mejores prácticas en cuanto a su desarrollo y al manejo de la información, se ha creado la Arquitectura TI Colombia, cuyo principal instrumento es el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI. Con él se busca habilitar las estrategias de Gobierno en línea de TIC para Servicios, TIC para la Gestión, TIC para el Gobierno Abierto y Seguridad y la Privacidad de la Información.

## 9. DESCRIPCIÓN DETALLADA DEL MODELO DE OPERACIÓN

En el presente capítulo se explica el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

***Ilustración 1 – Marco de Seguridad y Privacidad de la Información***



## 10. FASE- ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, que de ahora en adelante se denominará MSPI, el cual hace parte integral de la Estrategia de Gobierno en línea.

***Ilustración 2 – Etapas previas a la implementación***

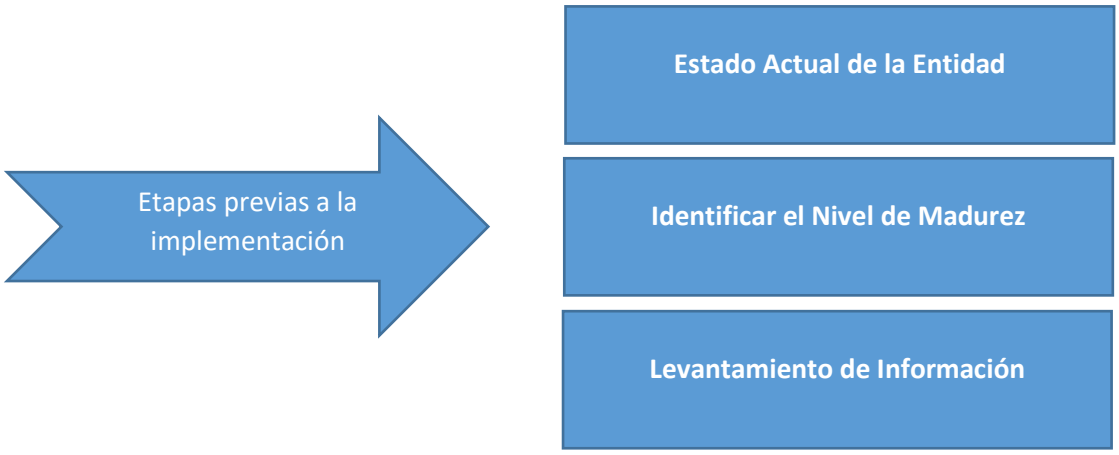



***Tabla 1 – Metas y Resultados de la Fase etapas previas a la implementación:***

| NIVEL DE MADUREZ: PREPARACIÓN | |
|---|---|
| **Metas** | ***Resultados*** |
| Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. | Documento con el resultado de la encuesta, revisado, aprobado y aceptado por la alta dirección. Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección. |
| Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad. | Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de seguridad y privacidad de la información. |
| Realizar levantamiento de información para las pruebas de efectividad que permitan a la Entidad medir los controles existentes. | Documento con la preparación para el análisis de vulnerabilidades y de riesgo. |

En la fase previa a la implementación del Modelo de Seguridad y Privacidad de la Información “MSPI”, se alcanzarán las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Para ello se pueden utilizar los siguientes instrumentos:

- **Encuesta de seguridad:** brinda a las entidades un conjunto de preguntas que les ayudan al levantamiento de la información de su infraestructura física, lógica y metodológica de seguridad, como parte del estudio de la situación actual de cada una de ellas.
- **Estratificación:** la estratificación de las entidades permite identificar de manera general, el nivel de complejidad que puede significar para estas, la implementación del MSPI.
- **Autodiagnóstico de cumplimiento de la ley de protección de datos personales:** le ayudará a la entidad a determinar el grado de adecuación frente a las obligaciones derivadas de la ley de datos personales.

➢ Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad. Tenga en cuenta el siguiente instrumento:

- Autoevaluación del Modelo de Seguridad de la Información: brinda un punto de partida a las entidades al realizar un diagnóstico de los requisitos del MSPI que se han desarrollado, de acuerdo al nivel madurez y los dominios de la norma ISO 27001:2013.

➢ Realizar levantamiento de información para las pruebas de efectividad que permitan a la Entidad medir los controles existentes.

- El resultado de la aplicación de los instrumentos de autoevaluación, encuesta, estratificación y autodiagnóstico, permitirá determinar el nivel de madurez de seguridad y privacidad de la información en la entidad y establecer la brecha con los objetivos a alcanzar.

- Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación.

- Los entregables asociados a las metas en la fase de etapas previas a la implementación deben ser revisados y aprobados por la alta Dirección.

## 11. FASE – PLANIFICACIÓN

Esta fase tiene la finalidad de generar un plan de seguridad y privacidad alineado con el propósito 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.

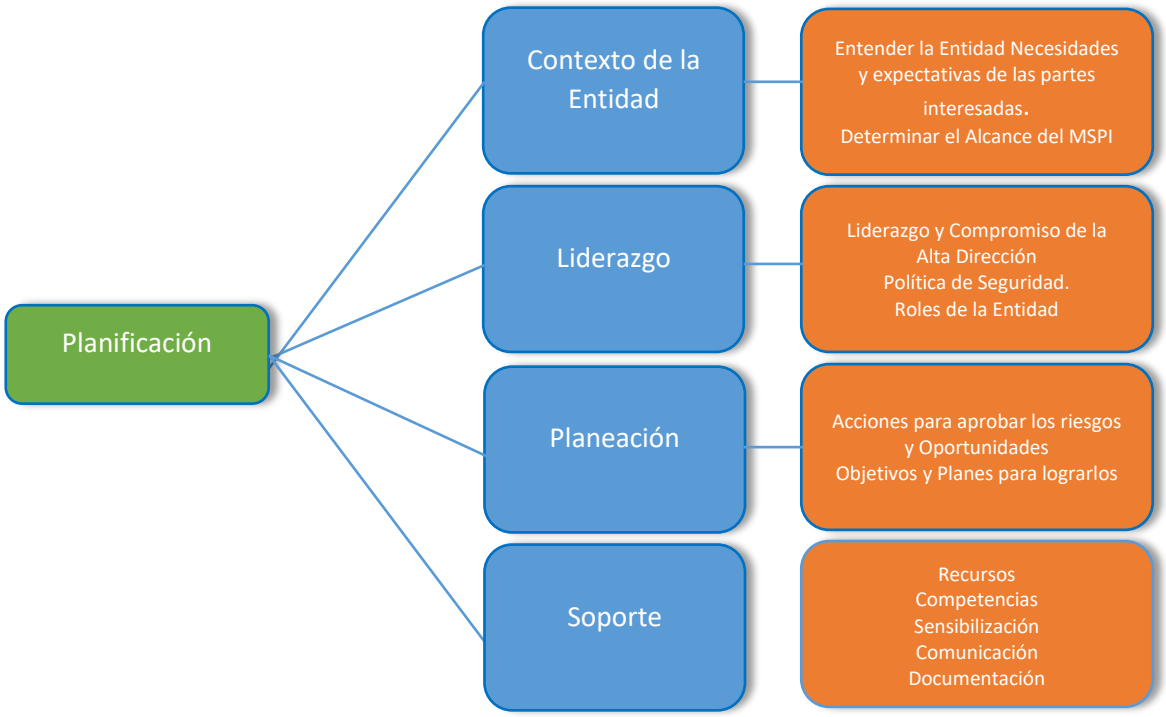



***Tabla 2 – Metas y Resultados de la Fase de Planificación:***

| NIVEL DE MADUREZ: DEFINIDO | |
|---|---|
| **Metas** | **Resultados** |
| **Política de seguridad general con Objetivos y alcance del MSPI.** | Documento con la política general de seguridad de la información, debidamente aprobado y socializado al interior de la Entidad, por la alta Dirección. |
| **Políticas de seguridad y privacidad de la información.** | Documentos con las políticas específicas de seguridad y privacidad de la información, debidamente aprobados y socializados al interior de la Entidad, por la alta Dirección. |
| **Procesos y procedimientos, debidamente definidos.** | Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional. |
| **Asignación de recurso humano, comunicación de roles y** | Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión |

| | |
|---|---|
| **responsabilidades de seguridad y privacidad de la información.** | 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. |
| **Inventario de activos de información.** | Documento con la identificación, clasificación y valoración de activos de información, revisado y aprobado por la alta Dirección. |
| **Integración del MSPI con el Sistema de Gestión documental.** | Plan de integración del MSPI y Sistema de Gestión Documental. |
| **Descripción de los flujos de los activos de tipo información que contengan datos personales.** | Documento con la caracterización del nivel de circulación de los activos tipo información que contengan datos personales. |
| **Acciones para tratar riesgos y oportunidades de seguridad de la información: identificación, valoración y tratamiento de riesgos.** | Documento con el informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad, revisado y aprobado por la alta Dirección. |
| **Toma de conciencia.** | Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. |

En este capítulo se explica de manera general como se debe avanzar en la fase de planificación del Modelo de Seguridad y Privacidad de la Información. Las metas a alcanzar son:

- ***Objetivos y alcance del MSPI.***

Los objetivos del MSPI están enmarcados en el cumplimiento de las propiedades de la seguridad de la información (confidencialidad, integridad y disponibilidad) en las entidades del Estado para garantizar sus objetivos misionales y necesidades propias. El alcance del MSPI permite a la E.S.E. Centro de Salud de Galapa, definir los límites sobre los cuales se implementará la seguridad y privacidad dentro de 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. El Alcance del Modelo de Seguridad y Privacidad de la Información debe incluir todos los procesos de la entidad.

- ***Políticas de seguridad y privacidad de la información***

La Política General de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Dirección de la Entidad para apoyar la

implementación del Modelo de Seguridad y Privacidad de la Información. La política general debe contener al menos una declaración general de compromiso por parte de la administración, sus objetivos, alcance, límites el nivel de cumplimiento, políticas específicas que soportan el SGSI. Así mismo es necesario tener en cuenta que las políticas específicas mínimas a implementar deben ser: Gestión de activos, control de acceso, no repudio, privacidad de la información, integridad, disponibilidad del servicio e información, registro y auditoría. Estas políticas deben ser aprobadas y divulgadas de tal forma que sean de obligatorio cumplimiento. Procesos y procedimientos, debidamente definidos. Los procedimientos asociados al Modelo deben ser implementados y utilizados dentro de las áreas de la Entidad, además deben ser aprobados por el Sistema de Gestión de Calidad.

Por otra parte, la guía Procedimientos de Seguridad de la Información muestra unos ejemplos de procedimientos mínimos que deberían implementar las Entidades relacionadas con controles de seguridad y privacidad de la Información.

Asignación del recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información.

Se deben definir los roles y responsabilidades de Seguridad y Privacidad de la información dentro de la Entidad a través de las siguientes actividades:

- Asignar responsabilidades generales y específicas, en las que se incluyan los roles (sin hacerlo para personas concretas dentro de la organización), con el apoyo de la guía roles y responsabilidades.
- Tratar los temas de seguridad de la información en los comités de gestión de la Entidad.
- Tratar los temas de seguridad de la información en los comités directivos de la Entidad.
- Inventario de activos de información.

Se debe desarrollar la metodología propuesta por la Guía de Clasificación de Activos de Información, teniendo en cuenta que el inventario de activos de información implica la clasificación y valoración de los mismos.

La clasificación debe verse desde el punto de vista técnico y de contenido de la información.

- ***Integración del MSPI con el Sistema de Gestión documental.***
- ***Descripción de los flujos de los activos de tipo información que contengan datos personales.***

A partir del inventario de activos de información la entidad debe poder determinar qué información contiene datos personales para determinar su tratamiento en función de la valoración hecha en el inventario.

- ***Acciones para tratar riesgos y oportunidades de seguridad de la información.***

  Utilizar una metodología de gestión del riesgo enfocada a procesos, para este caso se sugiere utilizar la metodología del Departamento Administrativo de la Función Pública – DAFP, que contiene los siguientes pasos:

- ***Identificación y valoración de riesgos de (Metodología, Reportes).***

- ***Tratamiento de riesgos (Selección de controles).***

- ***Toma de conciencia.***

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 costumbres en todos aquellos que tienen que ver con la seguridad de la información en las entidades.

Este plan será ejecutado, con el aval de la alta dirección, a todas las áreas de la Entidad. Para estructurar dicho plan puede utilizar la Guía para el plan de comunicación, sensibilización y capacitación.

Los resultados asociados a las metas en la Fase de Planificación deben ser revisados y aprobados por la alta Dirección.

## 12. FASE – PLANIFICACIÓN

Esta fase le permitirá a la Entidad, llevar a cabo la implementación de la planificación realizada en la fase de planificación del MSPI, teniendo en cuenta los aspectos más relevantes en los procesos de implementación del MSPI.

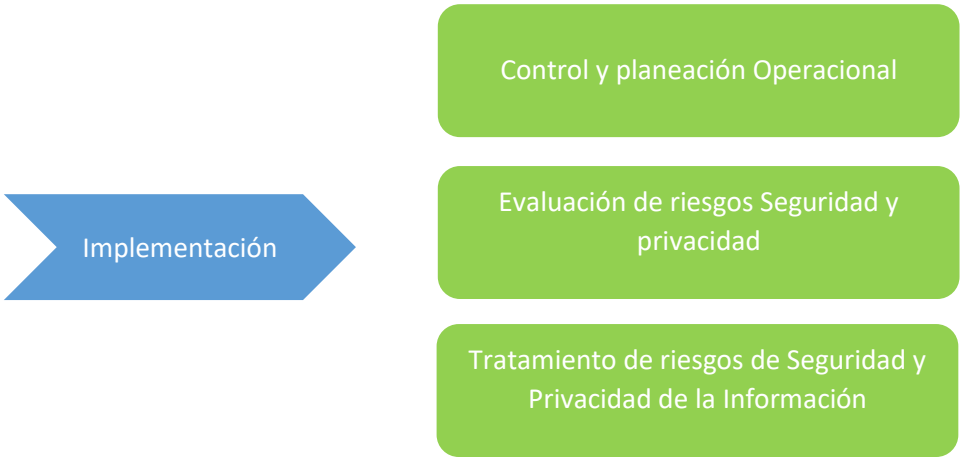



***Tabla 3 – Metas y Resultados de la Fase de Implementación:***

| **NIVEL DE MADUREZ: DEFINIDO** | |
|---|---|
| ***METAS*** | ***RESULTADOS*** |
| Plan de implementación | Documento con el plan de implementación revisado y aprobado por la alta Dirección. |
| Implementación del plan de tratamiento de riesgos. | Informe de la ejecución del plan de tratamiento de riesgos aprobado por los responsables de los procesos. |
| Plan de control operacional | Documento con el plan de control operacional revisado y aprobado por la alta Dirección, incluido el cronograma de actividades. |

Tomando como base en los resultados obtenidos en las fases de previas a la implementación y planificación del Modelo de Operación de Seguridad y Privacidad de la Información (MSPI), y de acuerdo con la identificación de las necesidades de la Entidad, se elabora el plan de Implementación y se ejecuta el plan de tratamiento de riesgos del MSPI.

- ***Plan de implementación***

La entidad debe planear, implementar y controlar los procesos misionales y de apoyo, validando la efectividad de los controles a implementar garantizando sus objetivos misionales. Dichos controles deben estar documentados y debe ser verificada su efectividad cada cierto tiempo. La entidad debe controlar que no se presenten cambios que afecten los procesos, tomando acciones para mitigar cualquier evento adverso, es decir se deben controlar sus procesos.

- ***Implementación del plan de tratamiento de riesgos.***

Se implementa 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, en donde la base para ejecutar esta fase es el anexo A de la Norma ISO 27001:2013 y la guía de controles sobre privacidad del MSPI. Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por los responsables de los procesos.

- ***Plan de control operacional***

Es el plan que debe construir la entidad para efectuar el monitoreo y seguimiento a los controles de seguridad definidos para los procesos. Los entregables asociados a las metas en la Fase de Implementación deben ser revisados y aprobados por la alta Dirección.

## 12. FASE – EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base en los resultados que arroja los indicadores de la seguridad de la información propuestos para verificación de la eficacia y efectividad de los controles implementados.

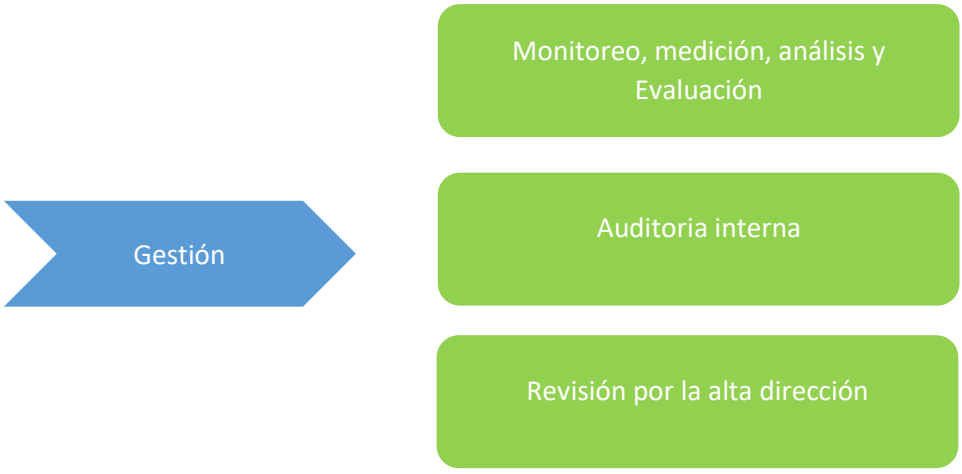


***Tabla 4 – Metas y Resultados de la Fase de Desempeño:***

| NIVEL DE MADUREZ: ADMINISTRATIVO | |
|---|---|
| **METAS** | **RESULTADOS** |
| Plan de seguimiento, evaluación y análisis del MSPI. | Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección. |
| Plan de ejecución de Auditoria Interna. | Resultados de la auditoria interna al MSPI, de acuerdo a lo establecido en el plan de auditoría, revisado y aprobado por la alta Dirección. |

Para definir el plan de seguimiento, evaluación y análisis del MSPI, se requiere dar respuesta a los siguientes interrogantes:

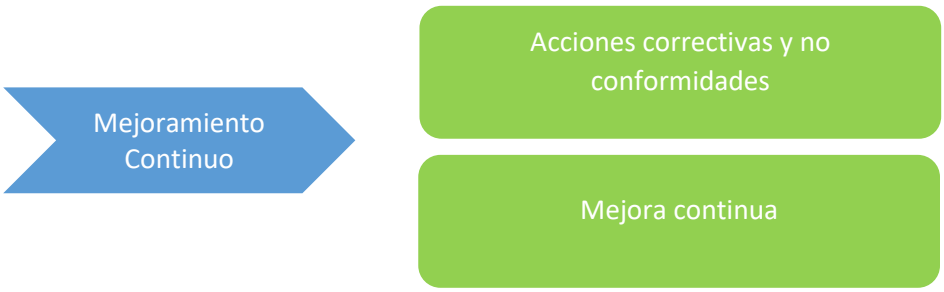
- ¿Qué actividades dentro del MSPI deben ser monitoreadas y evaluadas?
- ¿Qué acciones son necesarias para ese seguimiento y evaluación?
- ¿Quién es el responsable de las acciones de seguimiento y evaluación?
- ¿Cuándo se planifican las acciones de seguimiento y evaluación (oportunidad y periodicidad)?
- ¿Qué metodología se está usando para hacer seguimiento y evaluación del MSPI?
- ¿Qué recursos (financieros, humanos, técnicos, entre otros) se requieren para la ejecución del plan de seguimiento?

Nota: Difundir a los interesados los resultados de la evaluación del Plan de Seguridad de la Información, este tipo de actividad no debe confundirse con la difusión y concientización en seguridad de la información. La auditoría interna, es un procedimiento que se debe llevar a cabo para la revisión del MSPI implementado, de forma planificada con la finalidad de verificar que los

objetivos de control, controles, procesos y procedimientos del MSPI cumpla con los requisitos establecidos en la norma ISO 27002:2013 y los del MSPI. Los entregables asociados a las metas en la Fase de Evaluación del desempeño deben ser revisados y aprobados por la alta Dirección.

## 13. FASE – MEJORA CONTINUA

Esta fase le permitirá a la Entidad, 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, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.




En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

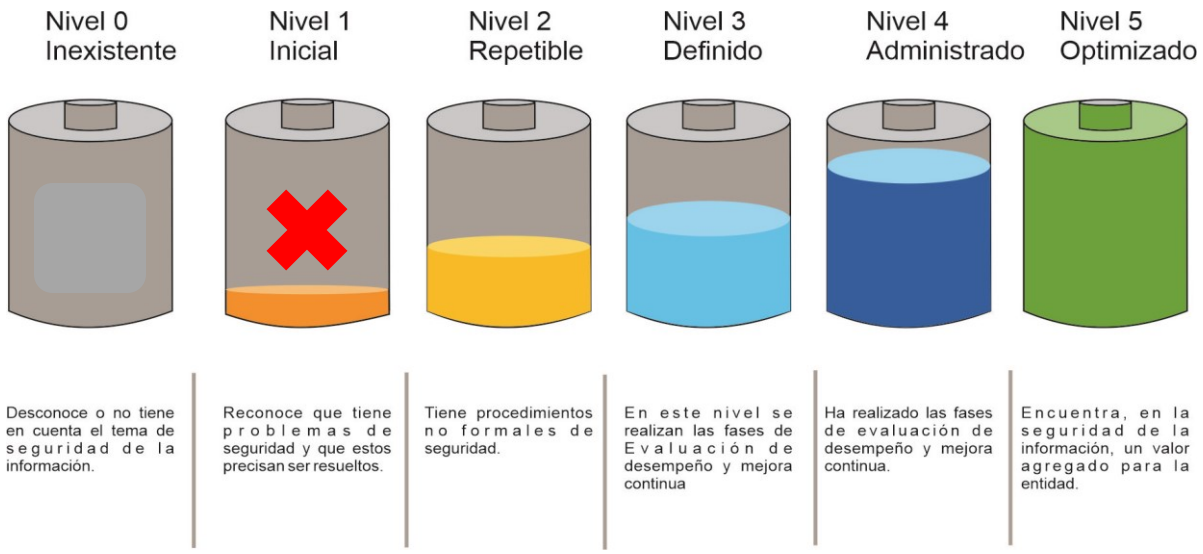
- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados de la auditoria interna al MSPI.

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 revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

## 14. MODELO DE MADUREZ

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

continuación, la ilustración 1, muestra los diferentes niveles que hacen parte del modelo de madurez.




El esquema que muestra los niveles de madurez del MSPI, busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en una entidad del Estado. En la tabla 1, se presentan los requerimientos de cada uno de los niveles de madurez con una descripción general.

***Tabla 6 – Descripción 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.<br>• No se tiene conciencia de la importancia de la seguridad de la información en las entidades. |
| **Inicial** | • Se han identificado las debilidades en la seguridad de la información.<br>• Los incidentes de seguridad de la información se tratan de forma reactiva.<br>• 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.<br>• Se clasifican los activos de información.<br>• Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.<br>• Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. |
| **Definido** | • La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.<br>• La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.<br>• La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.<br>• La Entidad tiene procedimientos formales de seguridad de la Información.<br>• La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.<br>• La Entidad ha realizado un inventario de activos de información aplicando una metodología.<br>• La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos |
| **Administrado** | • Se revisa y monitorea periódicamente los activos de información de la Entidad.<br>• Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.<br>• Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. |
| **Optimizado** | • En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.<br>• Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. |

## 15.PLAZOS

Los plazos para la implementación de las actividades se establecieron para el Manual de Gobierno en Línea, y a través del Decreto 2573 de 2014, en el Articulo 10. "Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierno en Línea dentro de los siguientes plazos:

### 15.1 Sujetos Obligados del Orden Territorial

a) Gobernaciones de categoría Especial y Primera; alcaldías de categoría Especial, y demás sujetos obligados de la administración publica en el mismo nivel.
b) Gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera y demás sujetos obligados de la Administración Pública en el mismo nivel.
c) Alcaldías de categoría cuarta, quinta y sexta y demás sujetos obligados de la Administración Pública en el mismo nivel.

Para las entidades agrupadas en C los plazos serán los siguientes:

| Componente/Año | Entidades C (%) | | | | | |
|---|---|---|---|---|---|---|
| | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 |
| TIC para ser servicios | 45% | 70% | 100% | Mantener 100% | Mantener 100% | Mantener 100% |
| TIC para Gobierno abierto | 65% | 80% | 100% | Mantener 100% | Mantener 100% | Mantener 100% |
| TIC para la Gestión | 10% | 30% | 50% | 65% | 80% | 100% |
| Seguridad y Privacidad de la Información | 10% | 30% | 50% | 65% | 80% | 100% |

## 16. GUÍAS MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los siguientes documentos se diseñados para un mejor entendimiento de las entidades en la implementación el Modelo de Seguridad y Privacidad de la Información.

| | NOMBRE | DESCRIPCIÓN |
|---|---|---|
| 1 | Encuesta de seguridad | Este documento presenta un conjunto de preguntas que ayuda al levantamiento de la información de la |

| | | |
|---|---|---|
| | | infraestructura física, lógica y metodológica de seguridad de las entidades, como parte del estudio de la situación actual de cada una de ellas. |
| 2 | Estratificación | Este documento presenta la estratificación de las entidades para la implementación del Modelo de seguridad. |
| 3 | Autoevaluación del Modelo de Seguridad y Privacidad de la Información | Este documento presenta un conjunto de herramientas de ayuda para auto diagnosticar de manera objetiva el nivel de implementación actual y da un listado de temas que componen la brecha con la seguridad de la información. |
| 4 | Metodológica de pruebas de efectividad | Este documento presenta una metodología para la planeación de las pruebas de efectividad. |
| 5 | Política general de seguridad y privacidad de la información | Este documento contiene una plantilla de política de seguridad de la información que las entidades pueden adaptar según sus objetivos estratégicos. |
| 6 | Procedimientos de Seguridad y Privacidad de la Información. | Este documento contiene una plantilla que le ayudara a construir procedimientos de seguridad de la información. |
| 7 | Roles y responsabilidades de seguridad y privacidad de la información | Este documento presenta los lineamientos a tener en cuenta en la inclusión de roles y responsabilidades (funciones y personal) en seguridad y privacidad de la información, que deben ser tratado en los comités directivos de gestión. |
| 8 | Identificación, clasificación y valoración de activos de información | Este documento presenta una metodología de clasificación de activos para las entidades del Estado en el marco del Programa Gobierno en línea. |
| 9 | Gestión documental del Archivo General de la Nación | Este documento ple proporciona una guía, de cómo debe manejar los archivos digitales de acuerdo con lo establecido en los decretos y guías del Archivo General de la Nación. |
| 10 | Gestión del riesgo | Este documento presenta una metodología para la gestión del riesgo al interior de las entidades del Estado en el marco del Programa de Gobierno en línea. |
| 11 | Controles de seguridad y Privacidad de la Información | Este documento presenta el conjunto de políticas que deben ser cumplidas por las entidades y 113 controles recomendados para que la entidad genere el documento de aplicabilidad de controles para el Sistema de Gestión de Seguridad de la Información. |
| 12 | Indicadores de gestión | Este documento presenta indicadores de seguridad y privacidad de la información, cuyo propósito es evaluar el estado de las entidades gubernamentales |

| | | |
|---|---|---|
| | | en materia de seguridad de la información, alineados con la Estrategia de Gobierno en línea. |
| 13 | Preparación de las TIC para la continuidad del negocio | En este documento encontrara los conceptos y principios para la preparación tecnología de información y comunicaciones (TIC), para la continuidad del negocio, y provee un marco de métodos y procesos que le permita identificar y especificar todos los aspectos para mejorar la preparación de las Entidades, para garantizar la continuidad del negocio. |
| 14 | Análisis de Impacto de Negocios (BIA) | Este documento, le guiara en la identificación y cuantificar el impacto de la perdida de funciones en la entidad. |
| 15 | Seguridad en la nube | Este documente presenta lineamientos para que las entidades incluyan dentro de sus estrategias cuales son las características de seguridad en la nube y como estructurar el desarrollo de la fase planificación del Modelo de Seguridad y Privacidad de la Información. |
| 16 | Evidencia digital | El presente documento da los lineamientos para realizar un proceso adecuado de informática forense, siendo a su vez un complemento al proceso de gestión de incidentes de seguridad de la información, ya que el enfoque de esta guía está relacionado con los eventos de seguridad de la información que pueden generar algún impacto a los activos de información. |
| 17 | Plan de comunicación, sensibilización y capacitación | Este documento tiene como objetivo establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cubra en su totalidad los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de las entidades del Estado. |
| 18 | Para definir el plan de implementación y plan de tratamiento de riesgos | Este documente presenta lineamientos para que las entidades sepan cómo estructurar el desarrollo de la fase de implementación y el plan de tratamiento de riesgos del Modelo de Seguridad y Privacidad de la Información. |
| 19 | Evaluación desempeño | Este documente presenta lineamientos para que las entidades sepan cómo estructurar el desarrollo de la fase de evaluación de desempeño del Modelo de Seguridad y Privacidad de la Información. |

| | | |
|---|---|---|
| 20 | Para efectuar auditoria del MSPI | Este documente presenta lineamientos para la ejecución de los auditorios referentes al Modelo de Seguridad y Privacidad de la Información. |
| 21 | Mejora continúa | Este documente presenta lineamientos para que las entidades sepan cómo estructurar el desarrollo de fase de mejora continua del Modelo de Seguridad y Privacidad de la Información. |
| 22 | Lineamientos: Terminales de áreas financieras entidades públicas | En este documento encontrará los lineamientos que las entidades deben implementar para elevar el aseguramiento de los equipos o terminales móviles asignados por la entidad, donde se realizan las transacciones a financieras como l os son: pago de nómina, pagos de seguridad social, pagos de contratación y transferencia as de fondos, entre otros. |
| 23 | Aseguramiento del protocolo IPv6 | Este documento presenta los lineamientos y consideraciones de seguridad que son necesarios tener en cuenta al momento de aplicar el protocolo IPv6 en cada una de las Entidades que entren a utilizar este nuevo protocolo. |
| 24 | | Este documento presenta la guía de acompañamiento para las entidades del Estado Colombiano, orientado a diagnosticar, desarrollar y aplicar las técnicas de transición de IPv4 a IPv6, mostrando las directrices en materia de equipamiento de computación y de comunicaciones necesarias para adoptar el protocolo IPv6, teniendo en cuenta los estándares que apoyan la transición del nuevo protocolo sobre las infraestructuras informáticas de TI, de las Entidades del Estado. |
| 25 | Gestión de incidentes | En este documento encontrara procesos de la gestión de incidentes, con el fin de mejorar la gestión de incidentes al interior de la Entidad. |

## 17. GUÍAS MARCO DE REFERENCIA DE ARQUITECTURA EMPRESARIAL

| LINEAMIENTO | DESCRIPCIÓN |
|---|---|
| Entendimiento estratégico | Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales cuando existan- y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos. |

| | |
|---|---|
| Definición de la Arquitectura Empresarial | Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución. |
| Políticas y estándares para la gestión y gobernabilidad de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: seguridad, continuidad del negocio, gestión de información, adquisición, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios. Así mismo, se debe contar con un proceso integrado entre las instituciones del sector que permita asegurar el cumplimiento y actualización de las políticas y estándares de TI. |
| Plan de comunicación de la estrategia | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir el plan de comunicación de la estrategia, las políticas, los proyectos, los resultados y los servicios de TI. |
| Participación en proyectos con componentes | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la institución que incorporen componentes de TI. Así mismo, debe asegurar la conformidad del proyecto con los lineamientos de la Arquitectura Empresarial definidos para la institución. |
| Control de los recursos financieros | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica el seguimiento y control de la ejecución del presupuesto y el plan de compras asociado a los proyectos estratégicos del PETI. |
| Gestión de proyectos de inversión | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe ser la responsable de formular, administrar, ejecutar y hacer seguimiento de las fichas de los proyectos de inversión requeridos para llevar a cabo la implementación de la Estrategia TI. El proceso de gestión de proyectos de inversión debe cumplir con los lineamientos que para este efecto establezca el Departamento Nacional de Planeación (DNP). |
| Evaluación de la gestión de la estrategia de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica la evaluación de la gestión de la Estrategia TI, para determinar el nivel de avance y cumplimiento de las metas definidas en el PETI. |
| Tablero de indicadores | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un tablero de indicadores sectorial |

| | |
|---|---|
| | y por institución, que permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI. |
| Alineación del gobierno de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución. |
| Conformidad | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir y realizar actividades que conduzcan a evaluar, monitorear y direccionar los resultados de las soluciones de TI para apoyar los procesos internos de la institución. Debe además tener un plan específico de atención a aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo de gestión, a fin de cumplir con el compromiso de mejoramiento continuo de la administración pública de la institución. |
| Cadena de Valor de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macro-proceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI. |
| Capacidades y recursos de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir, direccionar, evaluar y monitorear las capacidades disponibles y las requeridas de TI, las cuales incluyen los recursos y el talento humano necesarios para poder ofrecer los servicios de TI. |
| Criterios de adopción y de compra de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios y métodos que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la institución. Para todos los proyectos en los que se involucren TI, se deberá realizar un análisis del costo total de propiedad de la inversión, en el que se incorporen los costos de los bienes y servicios, los costos de operación, el mantenimiento, el licenciamiento, el soporte y otros costos para la puesta en funcionamiento de los bienes y servicios por adquirir. Este estudio debe realizarse para establecer los requerimientos de financiación del proyecto. Debe contemplar los costos de capital (CAPEX) y los costos de operación (OPEX). |
| Retorno de la inversión de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer la relación costo-beneficio y justificar la inversión de los proyectos de TI. Para establecer el retorno de la inversión, se deberá estructurar un caso de negocio para el proyecto, con el fin de asegurar que los recursos públicos se |

| | |
|---|---|
| | utilicen para contribuir al logro de beneficios e impactos concretos de la institución. Debido a la imposibilidad de obtener retorno monetario en algunos casos, ya que se trata de gestiones sin ánimo de lucro, los beneficios deben contemplar resultados de mejoramiento del servicio, de la oportunidad, de la satisfacción del ciudadano y del bienestar de la población, entre otros. |
| Liderazgo de proyectos de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas. La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá liderar el trabajo sobre el componente de TI conforme con los lineamientos de la Arquitectura Empresarial de la institución. |
| Gestión de proyectos de TI | El gerente de un proyecto, por parte de la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá evaluar, direccionar y monitorear lo relacionado con TI, incluyendo como mínimo los siguientes aspectos: alcance, costos, tiempo, equipo humano, compras, calidad, comunicación, interesados, riesgos e integración. Desde la estructuración de los proyectos de TI y hasta el cierre de los mismos, se deben incorporar las acciones necesarias para gestionar los cambios que surjan. |
| Indicadores de gestión de los proyectos de TI | El gerente de un proyecto, por parte de la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe monitorear y hacer seguimiento a la ejecución del proyecto, por medio de un conjunto de indicadores de alcance, tiempo, costo y calidad que permitan medir la eficiencia y efectividad del mismo. |
| Evaluación del desempeño de la gestión de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macroproceso de Gestión TI. |
| Mejoramiento de los procesos | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar áreas con oportunidad de mejora, de acuerdo con los criterios de calidad establecidos en el Modelo Integrado de Planeación y Gestión de la institución, de modo que pueda focalizar esfuerzos en el mejoramiento de los procesos de TI para contribuir con el cumplimiento de las metas institucionales y del sector. |
| Gestión de proveedores de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe administrar todos los proveedores y contratos para el desarrollo de los proyectos de TI. Durante el proceso contractual se debe aplicar un esquema de dirección, supervisión, seguimiento, control y recibo a satisfacción de los bienes y servicios contratados. |

| | |
|---|---|
| Transferencia de información y conocimiento | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe gestionar la transferencia de conocimiento asociado a los bienes y servicios contratados por la institución. Además, debe contar con planes de formación y de transferencia de conocimiento en caso de cambios del recurso humano interno. |
| Responsabilidad y gestión de Componentes de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir las directrices y liderar la gestión de los Componentes de información durante su ciclo de vida. Así mismo, debe trabajar en conjunto con las dependencias para establecer acuerdos que garanticen la calidad de la información. |
| Plan de calidad de los componentes de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un plan de calidad de los componentes de información que incluya etapas de aseguramiento, control e inspección, medición de indicadores de calidad, actividades preventivas, correctivas y de mejoramiento continuo de la calidad de los componentes. |
| Canales de acceso a los Componentes de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad. |
| Mecanismos para el uso de los Componentes de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe impulsar el uso de su información a través de mecanismos sencillos, confiables y seguros, para el entendimiento, análisis y aprovechamiento de la información por parte de los grupos de interés. |
| Acuerdos de intercambio de Información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer los Acuerdos de Nivel de Servicio (ANS) con las dependencias o instituciones para el intercambio de la información de calidad, que contemplen las características de oportunidad, disponibilidad y seguridad que requieran los Componentes de información. |
| Hallazgos en el acceso a los Componentes de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe generar mecanismos que permitan a los consumidores de los Componentes de información reportar los hallazgos encontrados durante el uso de los servicios de información. |
| Protección y privacidad de Componentes de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar, en los atributos de los Componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública. |

| | |
|---|---|
| Auditoría y trazabilidad de Componentes de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los Componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dicho Componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja. |
| Definición estratégica de los sistemas de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir la arquitectura de los sistemas de información teniendo en cuenta las relaciones entre ellos y la articulación con los otros dominios del Marco de Referencia. |
| Ambientes independientes en el ciclo de vida de los sistemas de información | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe disponer de ambientes independientes y controlados destinados para desarrollo, pruebas, operación, certificación y capacitación de los sistemas de información, y debe aplicar mecanismos de control de cambios de acuerdo con las mejores prácticas. |
| Seguridad y privacidad de los sistemas de información | En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información. |
| Auditoría y trazabilidad de los sistemas de información | En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios. |
| Continuidad y disponibilidad de los Servicios tecnológicos | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar que sus Servicios Tecnológicos estén respaldados con sistemas de alimentación eléctrica, mecanismos de refrigeración, soluciones de detección de incendios, sistemas de control de acceso y sistemas de monitoreo de componentes físicos que aseguren la continuidad y disponibilidad del servicio, así como la capacidad de atención y resolución de incidentes. |
| Alta disponibilidad de los Servicios tecnológicos | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar capacidades de alta disponibilidad que incluyan balanceo de carga y redundancia para los Servicios Tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente. |

| | |
|---|---|
| Acuerdos de Nivel de Servicios | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) para los Servicios Tecnológicos. |
| Planes de mantenimiento | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar un plan de mantenimiento preventivo sobre toda la infraestructura y los Servicios Tecnológicos. |
| Gestión preventiva de los Servicios tecnológicos | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurarse de que la infraestructura que soporta los Servicios Tecnológicos de la institución cuente con mecanismos de monitoreo para generar alertas tempranas ligadas a los umbrales de operación que tenga definidos. |
| Respaldo y recuperación de los Servicios tecnológicos | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un proceso periódico de respaldo de la configuración de sus Servicios Tecnológicos, así como de la información almacenada en la infraestructura tecnológica. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de los Servicios Tecnológicos. |
| Análisis de vulnerabilidades | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI. |
| Monitoreo de seguridad de infraestructura tecnológica | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar controles de seguridad para gestionar los riesgos asociados al acceso, trazabilidad, modificación o pérdida de información que atenten contra la disponibilidad, integridad y confidencialidad de la información. |
| Tecnología verde | La institución debe implementar un programa de correcta disposición final de los residuos tecnológicos, incluyendo las opciones de reutilización a través de otros programas institucionales con los que cuente el gobierno nacional. |
| Estrategia de Uso y apropiación | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de definir la estrategia de Uso y Apropiación de TI, articulada con la cultura organizacional de la institución, y de asegurar que su desarrollo contribuya con el logro de los resultados en la implementación de los proyectos de TI. |
| Matriz de interesados | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con una matriz de caracterización que identifique, clasifique y priorice los grupos de interés involucrados e impactados por los proyectos de TI. |
| Involucramiento y compromiso | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de asegurar el involucramiento y |

| | |
|---|---|
| | compromiso para llamar a la acción de los grupos de interés, partiendo desde la alta dirección hacia al resto de los niveles organizacionales, de acuerdo con la matriz de caracterización. |
| Esquema de incentivos | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de identificar y establecer un esquema de incentivos que, alineado con la estrategia de Uso y Apropiación, movilice a los grupos de interés para adoptar favorablemente los proyectos de TI. |
| Plan de formación | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de asegurar que el plan de formación de la institución incorpora adecuadamente el desarrollo de las competencias internas requeridas en TI. |
| Preparación para el cambio | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de elaborar un plan de gestión del cambio para facilitar el Uso y Apropiación de los proyectos de TI. Este plan debe incluir las prácticas, procedimientos, recursos y herramientas que sean necesarias para lograr el objetivo. |
| Evaluación del nivel de adopción de TI | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con indicadores de Uso y Apropiación para evaluar el nivel de adopción de la tecnología y la satisfacción en su uso, lo cual permitirá desarrollar acciones de mejora y transformación. |
| Gestión de impactos | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de administrar los efectos derivados de la implantación de los proyectos de TI. |
| Acciones de mejora | La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe diseñar acciones de mejora y transformación a partir del monitoreo de la implementación de su estrategia de Uso y Apropiación y de la aplicación de mecanismos de retroalimentación. |

## 18. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, 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 la norma técnica colombiana NTC ISO/IEC 27000 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.