Empresa Social del Estado
HOSPITAL SAN JUAN DE DIOS
BETULIA - SANTANDER

Modelo de Seguridad y Privacidad de la Información

Dr. Miguel René Tuta Rueda
Gerente

INTRODUCCION

El Modelo de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos. Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad.

Objetivo General

Generar el documento denominado Manual de Seguridad y Privacidad de la Información para la E.S.E. Hospital San Juan de Dios de Betulia, Santander.

Objetivos Específicos

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Optimizar la gestión de la seguridad de la información al interior de la E.S.E. Hospital San Juan de Dios de Betulia, Santander.
- Orientar a los ciudadanos en particular de la legislación relacionada con la protección de datos personales.
- Optimizar la labor de acceso a la información pública al interior de la E.S.E. Hospital San Juan de Dios de Betulia, Santander.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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

En el presente Modelo de Seguridad y Privacidad de la Información se contempla 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

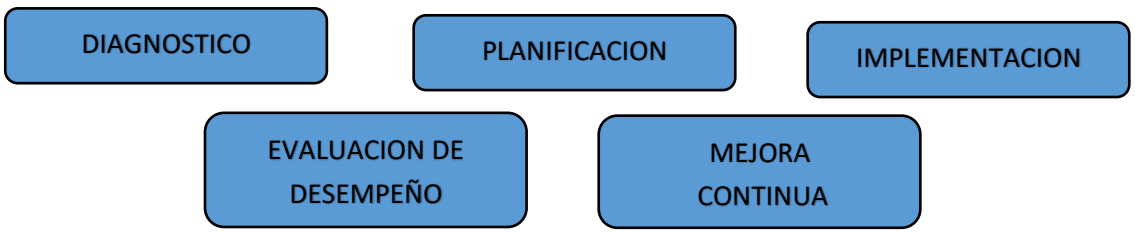
La seguridad y privacidad de la información, como componente transversal a la estrategia de Gobierno en Digital, permite alinearse al componente TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objeticos estratégicos de la entidad.

La seguridad y privacidad de la información se alinean 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 la protección de datos personales, así como otros derechos garantizados por la ley que exceptúa el acceso público a determinada información.

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

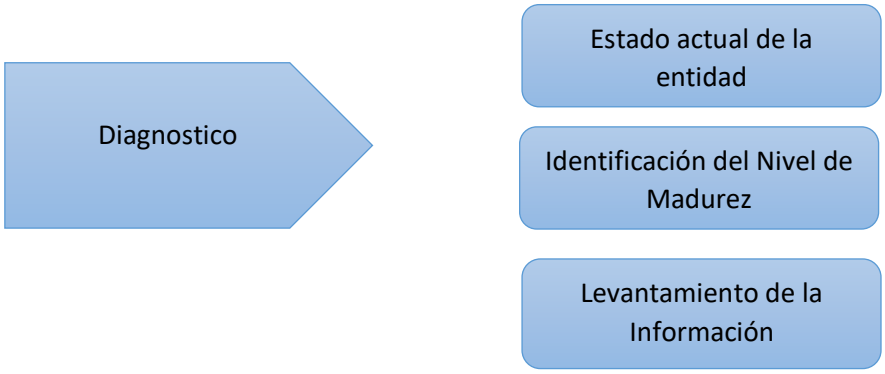
DESCRIPCION DEL CICLO DE OPERACIÓN

En el presente capitulo 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, herramientas que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.



1. FASE DE DIAGNOSTICO

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.



Instrumentos de la fase previa a la implementación:

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

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

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

Para ello se recomienda utilizar el instrumento denominado herramienta de diagnóstico.

Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad.

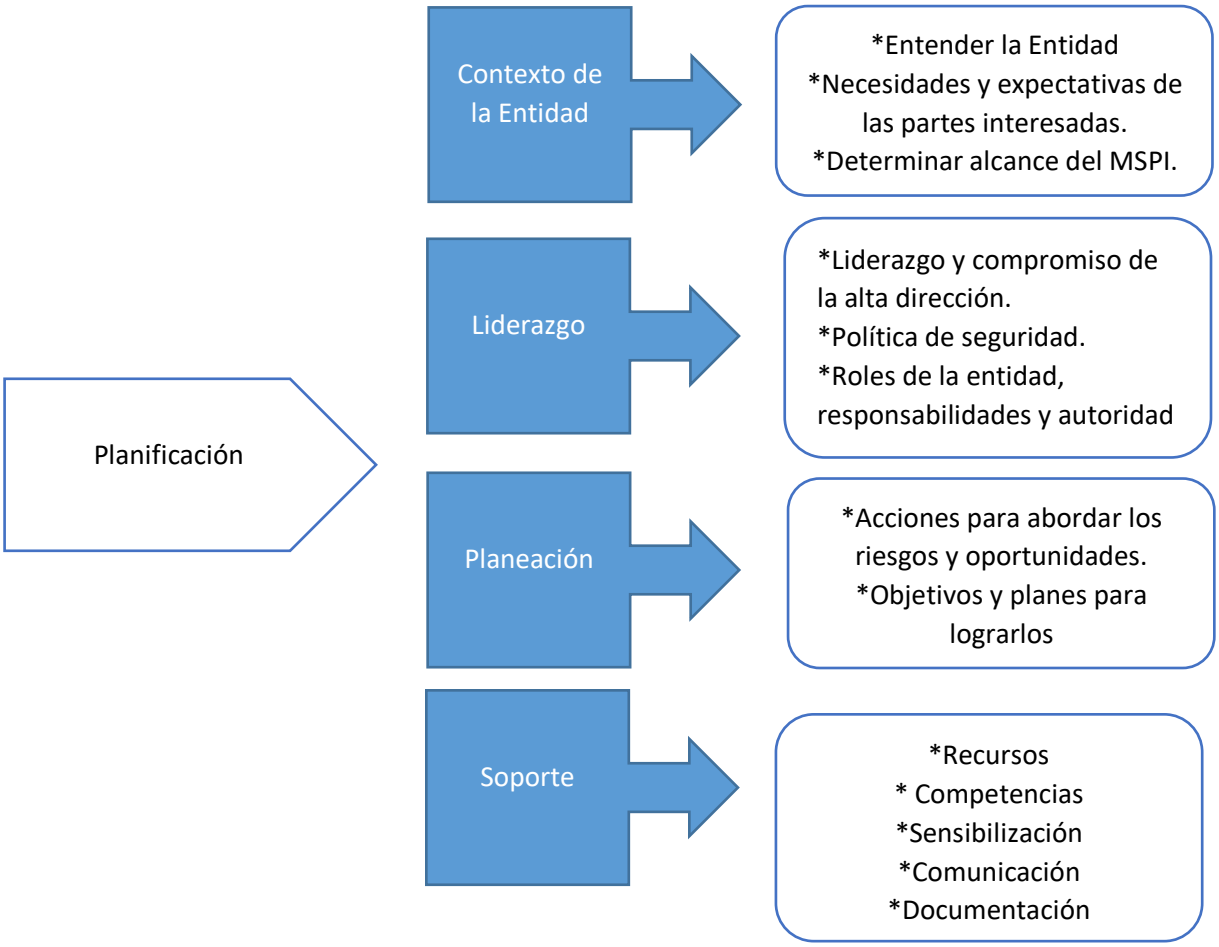
Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación.

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y asociados por las partes interesadas.

2. FASE DE PLANIFIACION

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

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



Metas	Resultados
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la entidad.
Procedimientos de Seguridad de la Información	Procedimientos debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional
Roles y responsabilidades de seguridad y privacidad de la información	Acto administrativo a través del cual se crea o se modifica las funciones del comité de gestión institucional, en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta dirección, deberá designarse quien será el encargado de la seguridad de la información dentro de la entidad.
Inventarios de activos de la información	Documento con la metodología para identificación, clasificación y valoración de activos informáticos, válido por el comité de seguridad de información o quien haga sus veces, revisado y aprobado por la alta dirección
Integración del MSPI con el Sistema de Gestión Documental	Integración del MSPI con el sistema de gestión documental de la entidad.
Identificación, valoración y tratamientos de Riesgo	Documento con la Metodología de Gestión del Riesgo Documento con la declaración de aplicabilidad. Documento revisados y aprobados por la alta dirección
Plan de Comunicaciones	Documento con el plan de comunicaciones, sensibilización y capacitación para la entidad.

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

Política de seguridad y privacidad de la información.

La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad del Gerente del Hospital de Betulia, para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. La Política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento, La política debe ser aprobada y divulgada al interior de la entidad.

Políticas de Seguridad y Privacidad de la Información

Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los activos de información al interior de la entidad, definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

Procedimientos de Seguridad de la Información

En este ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad, Para desarrollar esta actividad, la guía describe los procedimientos mínimos que se deben tener en cuenta para la gestión de la seguridad al interior de la entidad.

Roles y responsabilidades de Seguridad y Privacidad de la Información

La entidad debe definir mediante un acto administrativo los roles y responsabilidades de seguridad de la información en los diferentes niveles (Directivo, Procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la entidad, Para desarrollar estas actividades, la guía de roles y responsabilidades de la seguridad y privacidad de la información, brinda información relacionada para tal fin.

Inventario de activos de la Información

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

Integración del MSPI con el Sistema de Gestión Documental

La entidad deberá alinear la documentación relacionada con la seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el Archivo General de la Nación.

Identificación, valoración y tratamientos de riesgos

La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permitan identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que están expuestos los activos, así como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP- Departamento Administrativo de la Función Pública.

Plan de Comunicaciones

La entidad debe definir un Plan de Comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles de la Entidad de Salud.

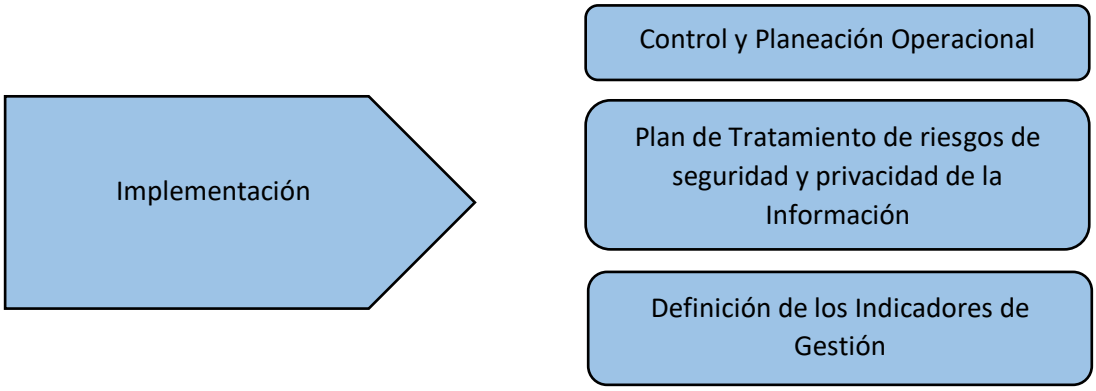
Este Plan será ejecutado, con el aval de la Alta Dirección a todas las áreas de la entidad.

Plan de transición de IPv4 a IPv6

Para llevar a cabo el proceso de transición del IPv4 a IPV6 en las entidades, se debe cumplir con la fase de planificación establecida en el soporte – guía.

3. FASE DE IMPLEMENTACION

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



Metas de Resultados e Instrumentos de la Fase de Implementación

IMPLEMENTACION	
Metas	Resultados
Planificación y Control Operacional	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta dirección.
Implementación de Plan de Tratamientos de Riesgos	Informe de la ejecución del plan de tratamiento de riesgo aprobado por el dueño de cada proceso.
Indicadores de Gestión	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.

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

Planificación y Control Operacional

La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el Plan de tratamientos de Riesgos, La entidad debe tener información documentada en la medida necesaria para tener la confianza en que los procesos de han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomas acciones para mitigar efectos adversos cuando sea necesario.

Implementación del Plan de Tratamientos de Riesgos

Se debe implementar el plan de tratamiento de riesgo de seguridad de la información, en el cual se identifica el control a aplicar para llevar a cabo uno de los riesgos a un nivel aceptable para la entidad. Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por el dueño de cada proceso.

Indicadores de Gestión

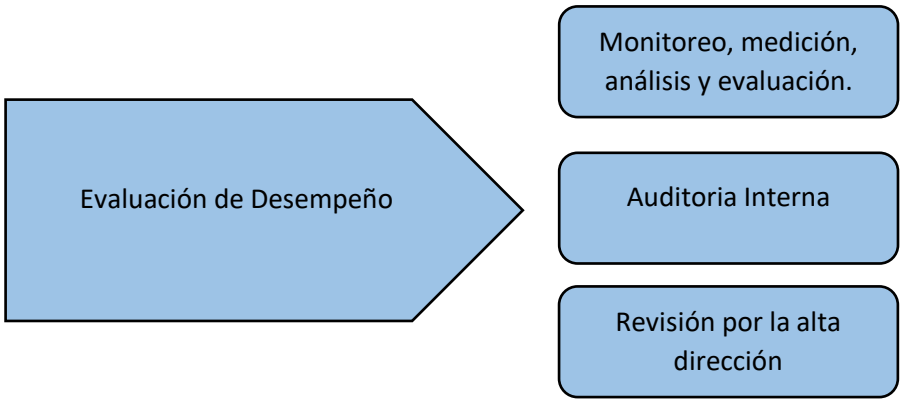
La entidad deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia de la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

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

4. FASE DE EVALUACION DE DESEMPEÑO

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



Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño.

IMPLEMENTACION	
Metas	Resultados
Planificación y Control Operacional	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta dirección.
Implementación de Plan de Tratamientos de Riesgos	Informe de la ejecución del plan de tratamiento de riesgo aprobado por el dueño de cada proceso.

Plan de revisión y seguimiento a la implementación del MSPI

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

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de los controles y medidas administrativas.

- Seguimiento a la programación y ejecución de las actividades de auditoría internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI.
- Revisiones de las acciones o planes de mejora.

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

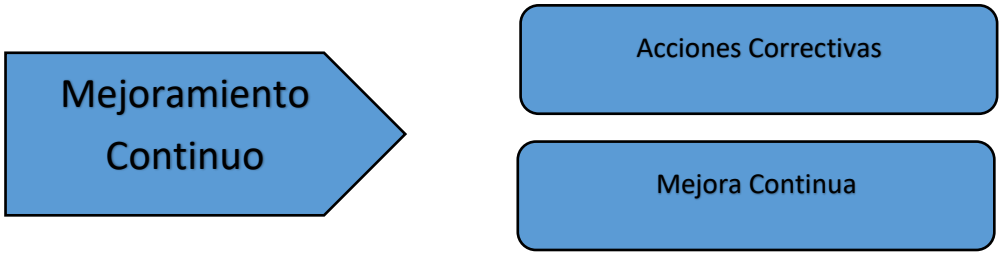
Plan de Ejecución de Auditorias

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

Se debe llevar a cabo las auditorias y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorias.

5. FASE DE MEJORA CONTINUA

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



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.

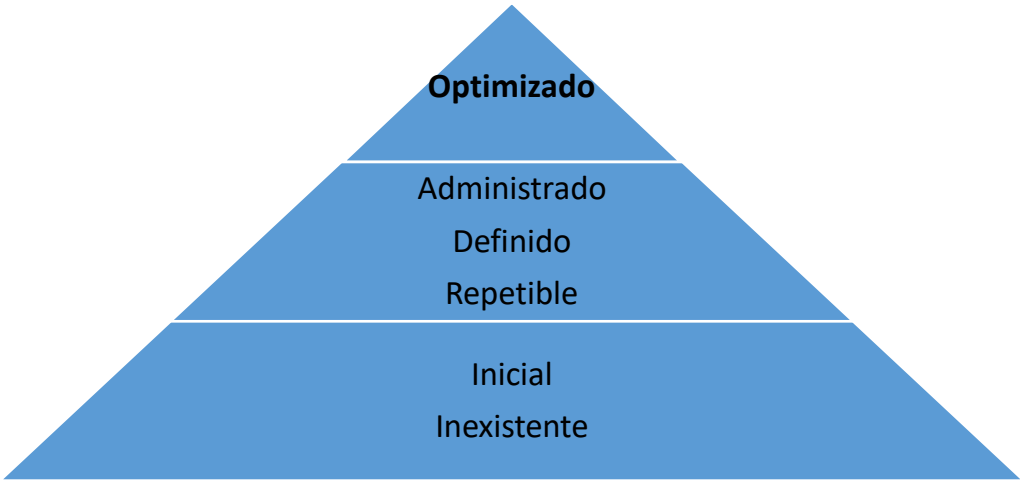
Este plan incluye

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

Utilizando los insumos anteriores, la entidad puede afectar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la alta dirección de la entidad. La revisión por la alta dirección hace referencia a las decisiones, cambios prioridades etc. Tomadas del comité y que impacten el MSPI.

MODELO DE MADUREZ

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



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.

PRIVACIDAD DE LA INFORMACION

Uno de los objetivos del modelo de seguridad y privacidad de la información es el de garantizar un adecuado manejo de la información pública en poder de las entidades destinatarias, la cual es uno de los activos más valiosos para la toma de

decisiones, el modelo propende por un doble enfoque a saber: a nivel de seguridad marcando un derrotero para que las entidades destinatarias construyan unas políticas de seguridad sobre la información a fin de salvaguardar la misma a nivel físico y lógico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad. En esta línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la administración como es el acceso a la información pública cuando esta no se encuentre sometida a reserva. Para ello se requiere dotar al modelo de seguridad de la información de un componente específico relacionado con la privacidad.

Para que los servidores públicos entiendan mejor el concepto de privacidad, hay que tener claro que diferentes procesos relacionados con la recolección y uso de información son susceptibles de ser objeto de implementación de medidas de privacidad, como puede ser:

- La implementación de un sistema de información que tenga la posibilidad de recolectar datos personales, tal como un sistema de seguridad a través de video vigilancia que capture imagines, datos biométricos, etc.
- El diseño y ejecución de un sistema de gestión documental.
- El desarrollo de políticas que implementen la necesidad de recolectar y usar información personal, como por ejemplo políticas de atención de PQRS.
- La transferencia de información a terceros.

Contar con una herramienta de análisis sobre el impacto en la privacidad

El MSPI es el instrumento que se pone a disposición de las entidades con el fin de realizar el análisis de impacto que en la privacidad de la información pueda presentar a partir del desarrollo de las funciones administrativas o el desarrollo misional de cada entidad. Teniendo como referente:

- El marco legal vigente
- Las necesidades de los clientes internos y externos de la entidad.
- La identificación de los posibles problemas recurrentes relacionados con la privacidad.

Descripción de los flujos de información

La descripción de los flujos de información sirve para saber qué información está siendo recolectada, con qué propósito, cómo, en qué cantidad y si la misma es objeto de divulgación.

La fase de diagnósticos de privacidad puede servir como insumo al poder identificar qué información se tiene, dónde y en cabeza de quien.

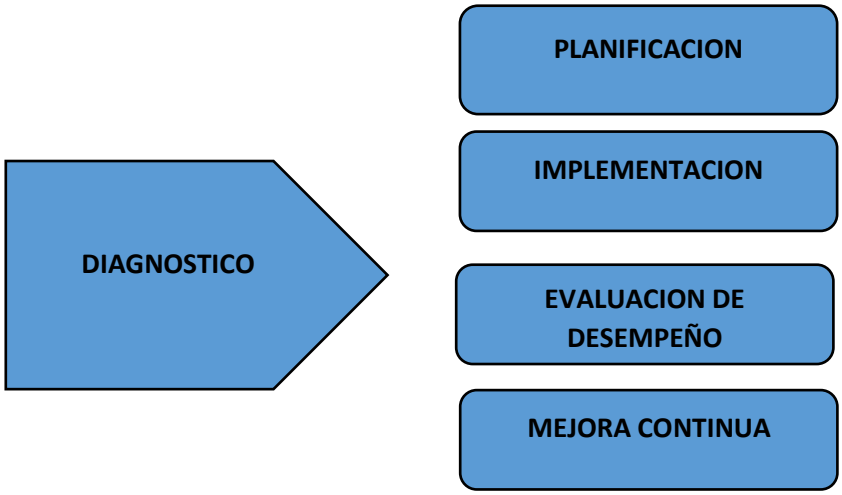
Identificar los riesgos de privacidad

Los riesgos en relación con la privacidad pueden ser de varios tipos:

- En relación con la información de personal de los individuos
  - Se expone información clasificada (Datos personales no públicos) son que medie autorización para ello.
  - Uso de sistemas de información o aplicaciones en la interacción con el ciudadano que pueden ser intrusivos sobre su privacidad son advertir previamente a usuarios sobre ellos (geolocalización).
  - Información que permanece en poder de la entidad por más tiempo de la vigencia que tiene la base de datos o en contra del ejercicio de derecho de suspensión por parte del titular – ciudadano.
- En relación con la información de usuarios institucionales
  - Se divulga información que puede ser clasificada como secreto industrial opone en riesgo la imagen corporativa.
- En relación con los sistemas de información y programas usados o los procedimientos y procesos relacionados con la gestión administrativa a cargo.
  - Procesos no ajustados al sistema de gestión documental que garanticen medidas de protección sobre la información.
  - Adquisición de programas que no garanticen un nivel adecuado de privacidad, por ejemplo que permite recolección masiva de datos sin conocimiento de los usuarios.
  - Indebida utilización de datos personales en ejercicios de divulgación tales como procesos de rendición de cuentas, publicación de información en la página web, etc.

El análisis debe reflejarse en una matriz de riesgos ponderando la probabilidad de su ocurrencia (ejemplo: baja – intermedia – alta) y el impacto que se debe generar su causación (Se sugiere utilizar una tabla numérica, por ejemplo – 1 ningún impacto a 10 impacto considerable)

La implementación del componente de privacidad sigue el mismo ciclo de operación adoptado para seguridad de la información consistente en cinco fases o etapas así: diagnostico, planeación, implementación, gestión y mejora continua.



FASE DIAGNOSTICO

En esta fase es necesario que las entidades identifiquen cómo se está garantizando la privacidad sobre todo el ciclo de la información que tiene en su poder verificando la implantación o no de medidas que den cumplimiento a los requerimientos de las normas sobre protección de datos personales y que adicionalmente contribuya a identificar la información pública sometida a reserva o clasificada en los términos de ley, Para ello se pone a disposición de las entidades, los instrumentos de diagnósticos y seguimiento a la implementación. A través del diligenciamiento de este instrumento se podrá conocer la realizada de la información relacionada con el manejo de los activos de la información que reposa en los bancos de datos o archivos y a partir de allí determinar las medidas a nivel procedimental que deben adelantar las entidades para otorgar un nivel adecuado de protección a esta información.

Metas, Resultados e Instrumentos de la Fase de Diagnostico

Con el resultado del diagnóstico se puede contar con un insumo frente a la identificación de aquella información que debe ser manejada como privada (Clasificada en los términos de ley) para a partir de allí incorporar las medidas de seguridad proporcionadas a su naturaleza como los procedimientos que lleven al cumplimiento de la normatividad de protección de datos.

Fase de Planificación

En esta segunda etapa se debe trazar la estrategia con el objetivo de organizar el trabajo adelantado por la entidad a partir de las características escogidas en la fase de diagnóstico, para acercarlas a un nivel de cumplimiento adecuado para salvaguardar la información privada y de manera concomitante responder a los retos

de disponibilidad a la información pública por parte de la ciudadanía, así como para ajustar los roles del personal designado para cumplir con las responsabilidades de seguridad y privacidad de a información.

Para ello deben ajustar las políticas, los procesos y procedimientos ya definidos en el modelo de seguridad con el fin de incorporar la privacidad con el alcance mencionado.

Planificación	
Metas	Resultados
Planificación	Documento con la Política de privacidad, debidamente aprobada por la alta dirección y socializada al interior de la entidad. Manual de políticas de seguridad y privacidad de la información, aprobada por la alta dirección y socializada al interior de la entidad. Documento con el plan de gestión de la privacidad sobre la información, aprobado por la alta dirección de la entidad. Definición de roles en relación con la información. Procedimiento de privacidad. Plan de capacitación al interior de la entidad.

Fase de Implementación

En esta fase se deben ejecutar las acciones trazadas en la etapa previa de planeación de manera que la entidad diseñe un modelo de privacidad que le permita cumplir con los mínimos legales y generar una política que le permita la correcta gestión de la Información.

De esta manera se da cumplimiento normativo, como: registro de bases de datos de información clasificada, reservada y revisada, procedimiento interno ajustado a la gestión de la privacidad de la información diseñada.

Implementación	
Metas	Resultados
Implementación	Documento con los riesgos contra la privacidad identificada y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información. Documento que se evidencia el registro de las bases de datos. Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados.

Fase de Evaluación y Desempeño

Una vez implementadas las anteriores actividades el modelo de privacidad se evalúa, para medir la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI y la aplicación de la Ley de Transparencia y Acceso de la Información Pública.

Evaluación de Desempeño	
Metas	Resultados
Evaluación del Desempeño	Documento con los resultados del plan de seguimiento. Documento con el Plan de Auditoria Interna y resultados revisado y aprobado por el Comité Institucional de Gestión y Desempeño. Comunicación de los indicadores al público a través de la rendición de cuentas.

Fase de Mejora Continua

Una vez tenga los resultados del componente de evaluación del desempeño se toman los resultados obtenidos y se preparan los correctivos necesarios que permitan a la misma crecer en el nivel de responsabilidad demostrada.

Adopción del Protocolo

En el presente capitulo se relacionan las fases para el proceso de transición del Protocolo IPv4 a IPv6 que orientará a las entidades del gobierno y a la sociedad en general en el análisis, la planeación y la implementación del protocolo IPv6.

Fase de Planeación

En esta fase, se debe definir el plan y la estrategia de transición del IPv6, en procura de los resultados que permitan dar cumplimiento con la adopción del nuevo protocolo.

En la tabla No. 10 se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad.

Metas, Resultados e Instrumentos de la Fase de Planeación

Planeación	
Metas	Resultados
Plan y estrategia de transición de IPv4 a IPv6	Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y Software) de cada entidad diagnosticada, informa de la infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, Plan de Direccionamiento en plan de manejo de excepciones, definiendo las acciones necesarias en caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean compatibles con IPv6, informe de preparación (Readiness) de los sistemas de comunicaciones bases de datos y aplicables. Documento que define la estrategia para la implementación y aseguramiento del protocolo IPV6 en concordancia con la política de seguridad de las entidades.

Fase de Implementación

En esta fase se realizaran actividades tales como habilitación del direccionamiento de IPV6, montaje, ejecución y corrección de configuraciones para pruebas piloto, activar las políticas de seguridad del IPV6, validar la funcionalidad de los servicios y aplicaciones de las entidades, entre otras.

En la Tabla se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad.

Implementación	
Metas	Resultados
Implementación del Plan y estrategia de transición del IPv4 a IPv6	Documento con el informe de implementación del Plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta dirección.

Fase Pruebas de Funcionalidad

En esta fase se hacen pruebas de funcionalidad y/o monitoreo de IPv6, en sistemas de información, de almacenamiento de comunicaciones y servicios, frente a las políticas de seguridad perimetral, de servidores de cómputo, equipos de comunicaciones, de almacenamiento, entre otros. Tener en cuenta que se debe elaborar un inventario final de los servicios y sistemas de comunicaciones, bajo el nuevo esquema de funcionamiento IPV6.

En la siguiente tabla se describen metas entregables e instrumentos que pueden ser utilizados para cumplir esta actividad, de conformidad.

Pruebas de Funcionalidad	
Metas	Resultados
Plan de pruebas de funcionalidad de IPV4 a IPV6	Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación. Acta de cumplimiento a satisfacción de la entidad respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidas durante la fase II de la implementación. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

PLAZOS

Los plazos para la implementación de las actividades se establecieron para el Manual de Gobierno en Digital, a través del Decreto 1078 de 2015, en el artículo 10 “Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierno en Digital dentro de los siguientes plazos:

En ese orden de ideas, se permite la E.S.E Hospital San Juan de Dios de Betulia, Santander, proyectar el Modelo de Seguridad y Privacidad de la Información. – MSPI.

MIGUEL RENE TUTA RUEDA
Gerente E.S.E Hospital San Juan de Dios de Betulia.

Proyecto	Diana Katerine Rueda Contratista MIPG	
Reviso	Oscar Josué Melo Sanabria Supervisor	