CONTROL DE REVISIONES			
	ELABORÓ	**REVISÓ**	**APROBÓ**
NOMBRE Y APELLIDO / CARGO	Profesionales oficina de Sistemas	Profesional Apoyo Calidad	Coordinador oficina de Sistemas
FIRMA			
FECHA	01/11/2020	01/11/2020	01/11/2020

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**MOTIVO DEL CAMBIO**	**DESCRIPCIÓN DEL CAMBIO**
1	01/11/2020		Se creó la primera versión del documento

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2020

INTRODUCCIÓN

El Hospital Regional de la Orinoquía ESE, adopta el modelo de seguridad y privacidad de la información, propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno Digital.

Este documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI planteado desde la Política de Gobierno Digital en su habilitador de Seguridad.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno Digital, 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.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la Política de Gobierno Digital.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección 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; de otro lado el MSPI especifica los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital: Arquitectura y Servicios Ciudadanos Digitales.

El presente modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

DEFINICIONES

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

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

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

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

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

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

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

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).

OBJETIVOS

OBJETIVO GENERAL

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad de la Información para el Hospital Regional de la Orinoquía ESE.

OBJETIVOS ESPECÍFICOS

- Utilizar el Modelo de Seguridad y Privacidad para las Entidades del Estado, que contribuya al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para la aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en el Hospital Regional de la Orinoquía ESE.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a los diferentes procesos del Hospital Regional de la Orinoquía ESE, en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Orientar a la entidad en la transición de IPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
- Orientar a la entidad en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.
- Orientar al Hospital Regional de la Orinoquía ESE, en las mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- Optimizar la labor de acceso a la información pública al interior de la entidad.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.
- Promover la toma de conciencia de los funcionarios, contratistas, terceros y demás partes interesadas, referente a la seguridad y privacidad de la información, mediante capacitaciones, boletines informativos y canales oficiales de comunicación.
- Identificar los activos de información y los controles a establecer para la protección de estos.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que 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 contemplan 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 Política de Gobierno Digital, 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.

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

DESCRIPCIÓN DEL CICLO 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 (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

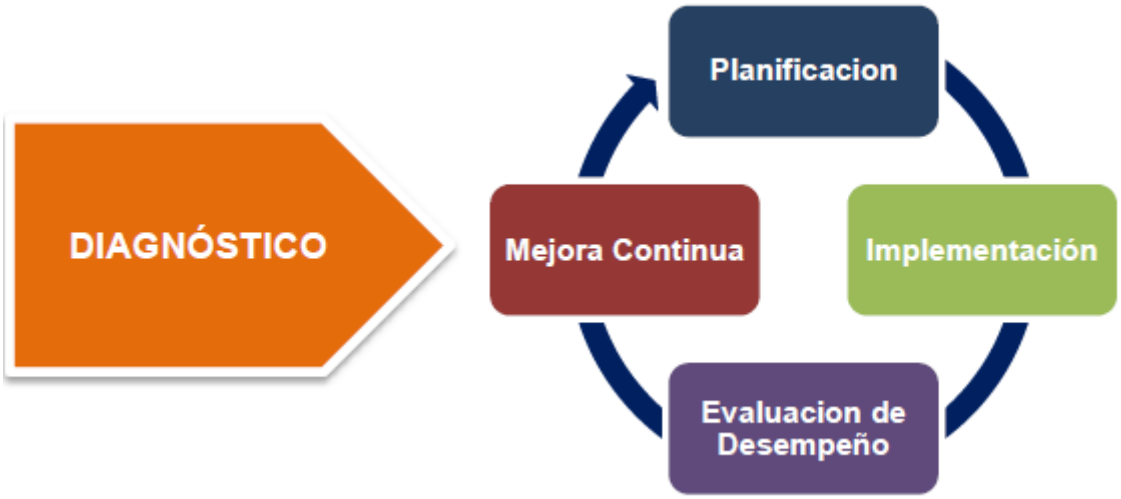

Imagen 1: Ciclo de operación del Modelo de Seguridad y Privacidad de la Información.

FASE DE DIAGNÓSTICO - 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.

Imagen 2: Etapas previas a la implementación.

INSTRUMENTOS DE LA FASE ETAPAS PREVIAS A LA IMPLEMENTACIÓN

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.
- Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.

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

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del Hospital Regional de la Orinoquía ESE.
- 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 del Hospital Regional de la Orinoquía ESE.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

FASE DE PLANIFICACIÓN

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

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

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

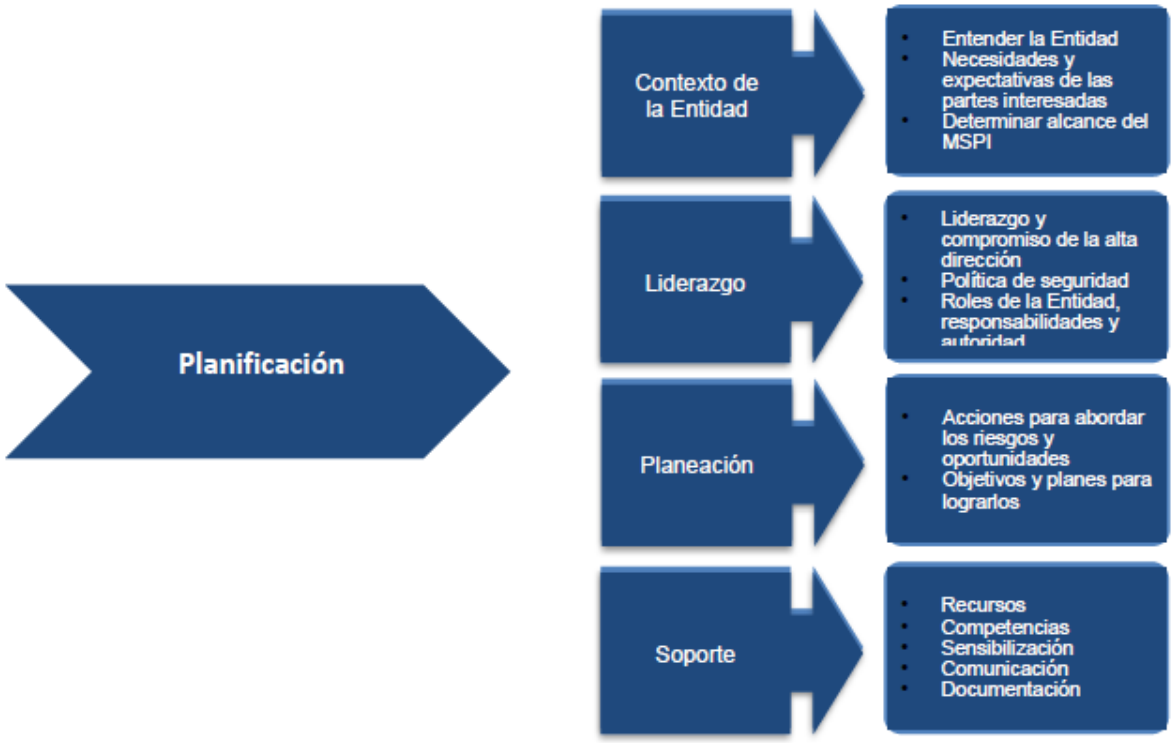

Imagen 3: Fase Planificación.

Metas y Resultados de la Fase de Planificación

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.
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad e integradas al PETI.
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 gestión institucional

	(o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

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 de la Alta Dirección de la Entidad 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 Específicas 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.

Basado en las guías y recomendaciones del MINTIC e igualmente en la norma NTC-ISO 27001:2013, se deben documentar los procedimientos de seguridad de la Información, ajustados al contexto del Hospital Regional de la Orinoquía ESE.

Roles y Responsabilidades de Seguridad y Privacidad de la Información.

El Hospital Regional de la Orinoquía ESE debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivos, Misionales y Administrativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

Inventario de activos de información.

El Hospital Regional de la Orinoquía ESE debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacta, actualizada y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios. Este inventario debe estar soportado por los instrumentos archivísticos, ajustado a la realidad de la entidad y acorde a la normatividad vigente en cuanto a clasificación de la información.

Integración del MSPI con el Sistema de Gestión documental.

El Hospital Regional de la Orinoquía ESE deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros establecidos por el archivo general de la nación y al Plan de Gestión Documental adoptado por la entidad.

Identificación, Valoración Y Tratamiento de Riesgos.

El Hospital Regional de la Orinoquía ESE debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, 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 respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad. Para definir la metodología, la entidad puede hacer uso de buenas prácticas vigentes tales como: ISO 27005, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos emitida por el MinTIC.

Plan de Comunicaciones.

El Hospital Regional de la Orinoquía ESE debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad. 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 de IPv4 a IPv6 en el del Hospital Regional de la Orinoquía ESE, se debe cumplir con las fases de diagnóstico, direccionamiento e implementación establecidas por el MINTIC.

FASE DE IMPLEMENTACIÓN

Esta fase le permitirá al Hospital Regional de la Orinoquía ESE, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

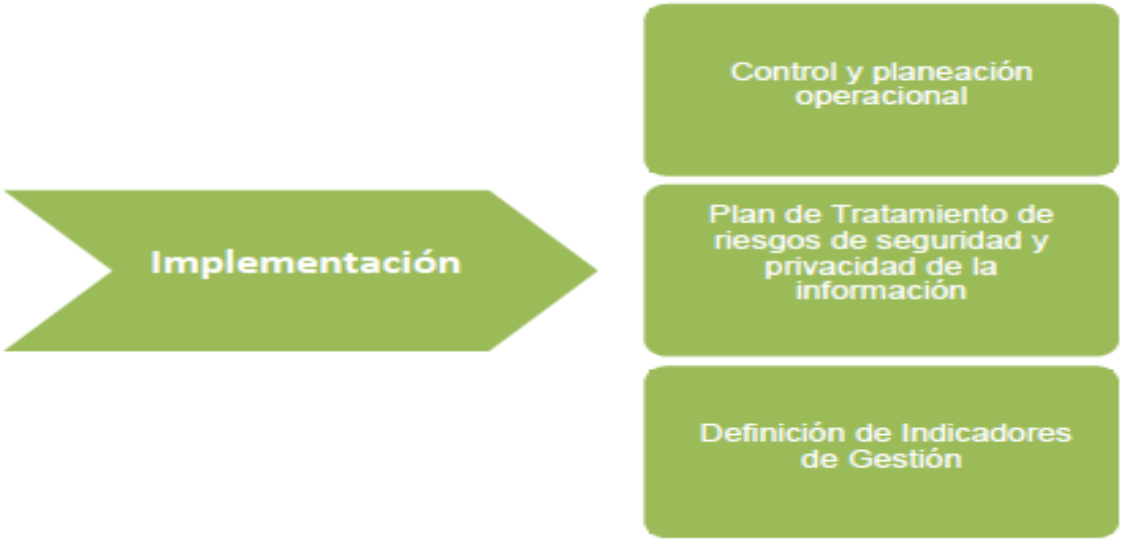

Imagen 4: Fase implementación.

Metas, Resultados e Instrumentos de la Fase de Implementación

METAS	RESULTADOS
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, 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 el dueño de cada proceso.
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Dirección de TIC.

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

Planificación y Control Operacional.

El Hospital Regional de la Orinoquía ESE debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

El Hospital Regional de la Orinoquía ESE debe tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

Implementación del plan de tratamiento de riesgos.

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

Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por el líder de cada proceso.

Indicadores De Gestión.

El Hospital Regional de la Orinoquía ESE deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

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

Plan de Transición de IPv4 a IPv6.

Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en el Hospital Regional de la Orinoquía ESE.

FASE DE EVALUACIÓN DE DESEMPEÑO

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

Imagen 5: Fase Evaluación de desempeño.

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

METAS	RESULTADOS
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

Plan de revisión y seguimiento a la implementación del MSPI.

En esta actividad el Hospital Regional de la Orinoquía ESE debe crear un plan que contemple las siguientes actividades:

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

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

Plan de Ejecución de Auditorias

El Hospital Regional de la Orinoquía ESE 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 auditorías 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 auditorías.

Es importante conservar la información documentada como evidencia de los resultados de las auditorías.

FASE DE MEJORA CONTINUA

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

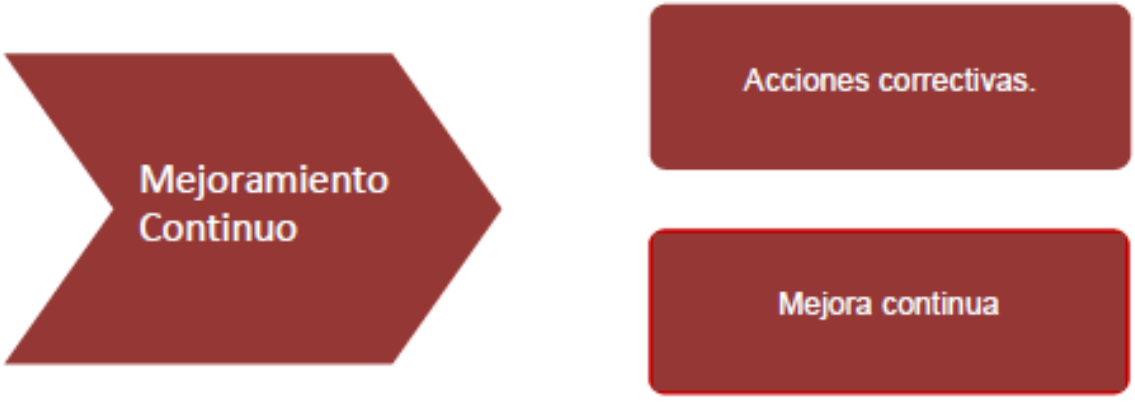

Imagen 6: Fase mejoramiento continuo.

Metas, Resultados e Instrumentos de la Fase de Mejora Continua

METAS	RESULTADOS
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.

En esta fase es importante que el Hospital Regional de la Orinoquía ESE 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, el Hospital Regional de la Orinoquía ESE puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

MODELO DE MADUREZ

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

Características de los Niveles de Madurez

NIVEL	DESCRIPCIÓN

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

	• La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. • La entidad genera tráfico en IPv6.

PRIVACIDAD DE LA INFORMACIÓN

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 distintas dependencias o unidades productoras que hacen parte del Hospital Regional de la Orinoquía ESE, 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 la entidad, construya 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 esa 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 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 imágenes, datos biométricos, etc.
- El Diseño y ejecución de un sistema de gestión documental.
- El Desarrollo de políticas que impliquen la necesidad de recolectar y usar información personal, como por ejemplo políticas de atención de PQR´s.
- La Transferencia de información a terceros (otras entidades o países).

Para ello la entidad debe tener en cuenta los siguientes temas.

Contar con una herramienta de análisis sobre 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 presentarse 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 diagnóstico de privacidad puede servir como insumo al poder identificar qué información se tiene, dónde y en cabeza de quién. Este ejercicio tiene que ser complementado con la documentación de los procesos relacionados con gestión de la información que la entidad haya levantado, para poder hacer una valoración sobre la circulación de la información, identificando que en la misma no se afecten derechos de los titulares de información o se ponga en riesgo su privacidad.

Identificar los riesgos de privacidad

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

- En relación con la información personal de los individuos
    - Se expone información clasificada (datos personales no públicos) sin que medie autorización para ello.
    - Uso de sistemas de información o aplicaciones en la interacción con los ciudadanos que pueden ser intrusivos sobre su privacidad sin advertir previamente a los usuarios sobre ello (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 supresión por parte del titular-ciudadano.
- En relación con la información de usuarios institucionales
    - Se divulga información que puede ser clasificada como secreto industrial o que pone 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 permitan 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 puede 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: diagnóstico, planeación, implementación, gestión y mejora continua.

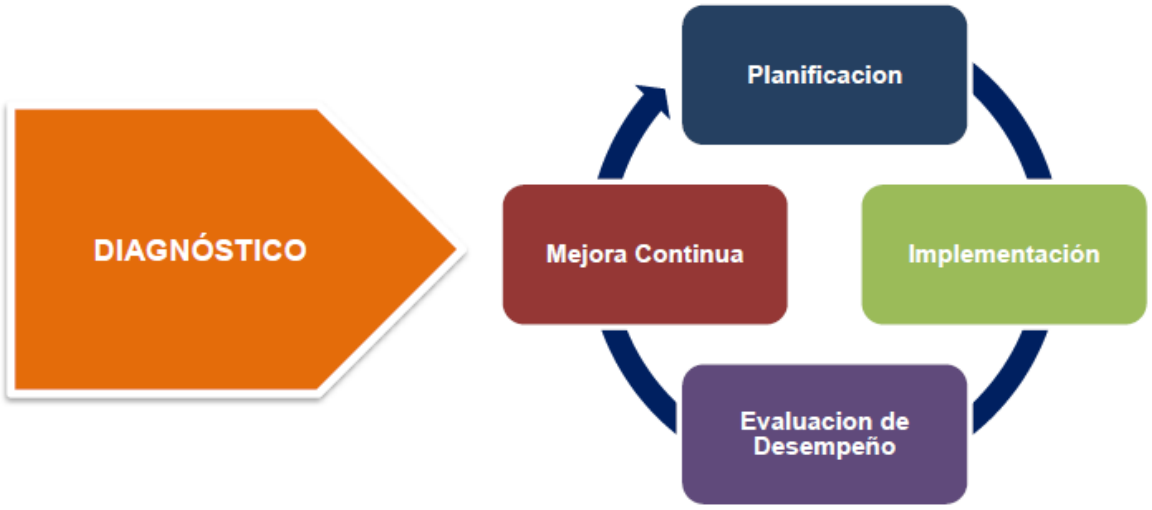

Imagen 7: Ciclo operación privacidad.

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 tienen 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 la Ley.

Para ello se pone a disposición de las entidades, el instrumento de diagnóstico y seguimiento a la implementación. A través del diligenciamiento de este instrumento se podrá conocer la realidad de la información relacionada con el manejo de los activos de la información que reposen en 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

METAS	RESULTADOS
Diagnostico	Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad. Diligenciamiento de la herramienta.
	Documento con el resultado del diagnóstico realizado por la entidad con la clasificación y distinción de los activos de información teniendo en cuenta la información con datos personales y aquellos que no lo son identificando la criticidad de la información clasificada o reservada.

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 la Ley) para a partir de allí incorporar las medidas de seguridad proporcionales a su naturaleza como los procedimientos que lleven al cumplimiento de la normatividad de protección de datos, transparencia y acceso a la información pública soportado todo ello en la incorporación de un sistema de privacidad por diseño que responda a la realidad presupuestal, humana y técnica de cada entidad.

Fase 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 recogidas 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 la información.

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

Metas, Resultados e Instrumentos de la Fase de 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. • Procedimientos 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 privacidad que le permita la correcta gestión de la información.
De esta manera se da cumplimiento normativo, como: registro de bases de datos en el RNBD, índice de información clasificado y reservado revisado, procedimiento interno ajustado a la gestión de la privacidad de la información diseñada.

Metas, Resultados e Instrumentos de la Fase de Implementación

METAS	RESULTADOS
Implementación	• Documento con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información. • Documento que evidencie el registro de las Bases de datos. • Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados.

Fase de Evaluación del 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 a la Información Pública.

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

METAS	RESULTADOS
Evaluación del desempeño	• Documento con los resultados del plan de seguimiento. • Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces. • Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.

Fase de Mejora Continua

Una vez se tengan 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.

Metas, Resultados e Instrumentos de la Fase de Mejora Continua

METAS	RESULTADOS
Mejora Continua	• Documento con los resultados del plan de seguimiento. • Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces. • Documento con el consolidado de las auditorias.

ADOPCIÓN DEL PROTOCOLO IPv6

En el presente capitulo se relacionan las fases para el proceso de transición del protocolo IPv4 a IPv6 que orientará a el Hospital Regional de la Orinoquía ESE en el análisis, la planeación y la implementación del protocolo IPv6.

Imagen 8: Fases del proceso de transición del protocolo IPv4 al IPv6.

FASE DE PLANEACIÓN

En esta fase, se debe definir el plan y la estrategia de transición de IPv4 a IPv6, en procura de los resultados que permitan dar cumplimiento con la adopción del nuevo protocolo.

Metas, Resultados e Instrumentos de la Fase de 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) diagnosticada, Informe 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 IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones. • Documento que define la estrategia del Hospital Regional de la Orinoquía ESE para la implementación y aseguramiento del protocolo IPv6 en concordancia con la política de seguridad de la entidad.

FASE DE IMPLEMENTACIÓN

En esta fase se realizan actividades tales como habilitación del direccionamiento de IPv6, montaje, ejecución y corrección de configuraciones para pruebas piloto, activar las políticas de seguridad de IPv6, validar la funcionalidad de los servicios y aplicaciones del Hospital Regional de la Orinoquía ESE, entre otras.

Metas, Resultados e Instrumentos de la Fase de Implementación

METAS	RESULTADOS
Implementación del plan y estrategia de transición de IPv4 a IPv6.	• Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

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 servicios y sistemas de comunicaciones, bajo el nuevo esquema de funcionamiento de IPv6.

Metas, Resultados e Instrumentos de la Fase de 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 del Hospital Regional de la Orinoquía ESE con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

Cronograma

El Plan de implementación para el Modelo de Seguridad y Privacidad de la Información del Hospital Regional de la Orinoquía ESE, comprende el siguiente cronograma y se le hará seguimiento cada vez que el comité de gestión y desempeño se reúna.

Actividad	Responsables	Fechas	
		Inicio	Final
Realizar diagnostico del estado actual, identificación del nivel de madurez y levantamiento de información del Hospital Regional de la Orinoquia, utilizando el instrumento de evaluación del MSPI.	Dirección de TIC	Diciembre 2020	Diciembre 2020

Levantar inventario de activos de información del Hospital Regional de la Orinoquia según lineamientos vigentes. Inventario de activos de IPv6	Dirección de TIC y Gestión Documental	Enero 2020	Diciembre 2021
Generación de documento con la Política General de Seguridad y Privacidad de la Información aprobado por la alta Dirección y socializada al interior de la Entidad.	Dirección de TIC	Enero 2021	Febrero 2021
Creación del Manual con las políticas específicas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Dirección de TIC	Febrero 2021	Mayo 2021
Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Dirección de TIC, Calidad	Mayo 2021	Noviembre 2021
Emitir acto administrativo a través del cual se crea o se modifica las funciones del comité gestión y desempeño (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Gerencia, Planeación, Calidad, Jurídica, Dirección TIC, Gestión Documental	Septiembre 2021	Septiembre 2021
Crear Documento con el plan de tratamiento de riesgos.	Dirección de TIC	Diciembre 2020	Febrero 2021
Documento con la declaración de aplicabilidad de los controles del Anexo A de la norma NTC-ISO 27001:2013	Dirección de TIC	Diciembre 2021	Marzo 2022
Documento con el análisis y evaluación de riesgos	Dirección de TIC	Enero de 2022	Junio de 2022

Documentos revisados y aprobados por la alta Dirección.	Gerencia, Planeación, Jurídica, Calidad, Gestión Documental, Dirección de TIC	Noviembre 2022	Noviembre 2022
Crear documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Dirección de TIC	Diciembre 2022	Diciembre 2022
Crear documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Dirección de TIC	Noviembre 2020	Marzo 2021