MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Proceso de Requerimientos Tecnológicos

2023

INTRODUCCION

El Modelo de Seguridad y Privacidad de la Información – MSPI, tiene el propósito de preparar a la Entidad para la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo que brinde confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Con la implementación de un modelo de seguridad y privacidad de la información, el Instituto del Desarrollo de Arauca - IDEAR, busca garantizar el cumplimiento de los objetivos esenciales y la misión institucional. Esto incluye la transparencia misma de la gestión pública, y el establecimiento establecer los lineamientos para adoptar las mejores prácticas de seguridad para prevenir incidentes con un impacto negativo, identificando la infraestructura crítica en la entidad. Promueve además un mejor intercambio de la información pública, cumplir con la legislación relacionada con la protección de datos personales, logrando respetar los derechos de los titulares de los datos (privacidad) y optimizando la labor de acceso a la información pública

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.

Este documento se elaboró siguiendo los lineamientos del Ministerio de las TIC en el marco de la estrategia de TI, denominado Modelo de Seguridad y Privacidad de la Información, el cual contiene la recopilación de las mejores prácticas nacionales e internacionales para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del MSPI; así mismo para estar acorde con las buenas prácticas de seguridad, se tomó como referencia un conjunto de documentos asociados al modelo que tiene disponible el Ministerio de las tic.

Para el desarrollo de cada uno de los productos y entregables de las diferentes etapas del ciclo de vida del MSPI, se toma como referencia las guías e instructivos dispuestos por el Ministerio de las TIC así como los documentos del marco de referencia de Arquitectura Empresarial.

1. OBJETIVOS

1.1 Objetivo General

Establecer las políticas, procedimientos y controles para garantizar la administración,manejo y control de la seguridad y privacidad de la información del Instituto de Desarrollo de Arauca – IDEAR.

1.2 Objetivos Específicos

- ✓ Brindar lineamientos para la implementación de la gestión de la seguridad y privacidad de la información.
- ✓ Asignar roles y responsabilidades para garantizar la seguridad y privacidad de la información.
- ✓ Promover el uso de mejores prácticas de seguridad de la información.
- ✓ Alinear el Modelo de Seguridad y Privacidad de la Información con el Marco de Referencia de Arquitectura Empresarial de TI. "PETIC Y Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información".
- ✓ Dar lineamientos para la implementación de mejores prácticas de seguridad que garanticen la privacidad, confidencialidad y disponibilidad de la información.
- ✓ Orientar a la Entidad para la construcción de una política de privacidad respetuosa de los datos personales de los clientes.
- ✓ Optimizar la gestión de la información al interior de la entidad.
- ✓ Contribuir al incremento de la transparencia en la gestión pública.
- ✓ Administrar los riesgos de seguridad digital a fin de incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información de la Entidad.

2. Modelo de Seguridad y Privacidad de la Información - MSPI

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, que permiten una adecuada gestión de la seguridad y privacidad de los activos de información.

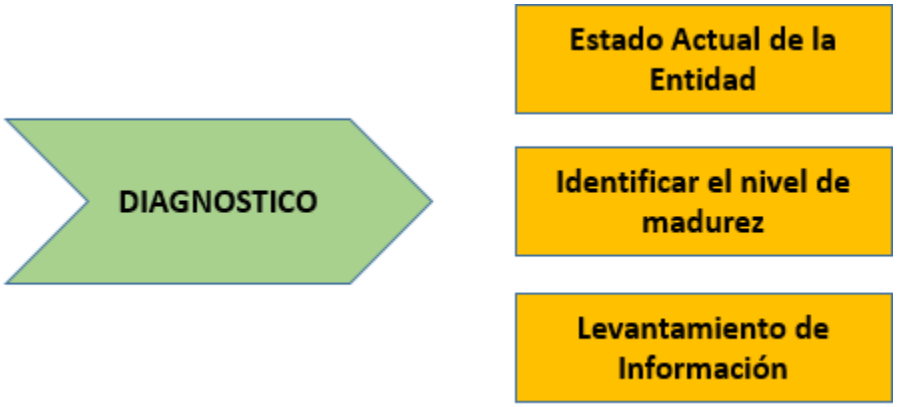
Figura 1. **Ciclo de operación Modelo de Seguridad y Privacidad de la Información**

3. Desarrollo del Ciclo de Operación

3.1 Diagnóstico

En esta fase se identifica el estado actual del Instituto de Desarrollo de Arauca - IDEAR, con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, y para tal efecto se utiliza la herramienta "Instrumento de Evaluación MSPI", suministrada por el Ministerio de las TIC para efectuar el autodiagnóstico.

El "Instrumento de Evaluación MSPI" es una herramienta que fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones, con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de laInformación".



Etapas Previas a la Implementación

En la fase de diagnóstico del MSPI se pretende:

- ✓ Determinar el estado actual de la gestión de seguridad y privacidad de lainformación al interior de la Entidad.
- ✓ Determinar el nivel de madurez de los controles de seguridad de la información.(ver Figura 7.)
- ✓ 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 en ciberseguridad.

En esta etapa se tomarán como documentos fuente, los instrumentos suministrados por el Ministerio de las TIC:

- ✓ Instrumento de evaluación MPSI.
- ✓ Instructivo para el diligenciamiento de la herramienta.
- ✓ Guía No 1 - Metodología de Pruebas de Efectividad.

Tabla 1 – Metas, Resultados e Instrumentos de la fase etapas previas a la implementación.

Nivel de Madurez: Preparación		
Metas	**Resultados**	**MSPI**
Determinar el estado actual de la gestión de seguridad y privacidad de la informaciónal interior de la Entidad.	Diligenciamiento de laherramienta de autoevaluación	Instrumento de EvaluaciónMSPI
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificacióndel nivel de madurez de la entidad.	Instrumento de EvaluaciónMSPI
Levantamiento de información para las pruebas que permitan establecer la efectividad de los controles existentes.	Documento con la preparación para el análisisde vulnerabilidades y de riesgo.	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 socializados por las partes interesadas.

3.2 Planificación

Basados en los resultados de la etapa anterior, se procede a la elaboración el plan de 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.

Basados en los resultados de la etapa anterior, se procede a la elaboración del plan de tratamiento de riesgos 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.

Tabla 2 – Metas - Resultados e Instrumentos de la fase de planificación

Metas	**Resultados**	**MSPI**
Política de Seguridad general con objetivos yalcance de MSPI	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – PolíticaGeneral MSPI.
Políticas de seguridad yprivacidad de la información	Documento con las políticas específicas seguridad y privacidad de la información, debidamenteaprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía No 2 - PolíticaGeneral MSPI.
Fases de Planificación		
Procesos y Procedimientosde seguridad de la información debidamente definidos	Formatos de procesos y Procedimientos, debidamente definidos, establecidos y aprobados por el comité de gestión institucional.	Guía No 3 - Procedimientosde Seguridad y Privacidad de la Información.

Roles y responsabilidadesde seguridad y privacidadde 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, revisadoy aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad dela información.
Inventario de activos deinformación.	Documento con la identificación, clasificación y valoración de los activos deinformación, revisado y aprobado por la alta Dirección.	Guía No 5 - Gestión De Activos
Integración del MSPI con elSistema de Gestión documental	Plan de Integración del MSPI y sistema de gestión documental de la entidad.	Guía No 6 - GestiónDocumental
Identificación, Valoración ytratamiento de riesgo.	Documento con la metodología de gestiónde riesgos. Documento con el análisis y evaluación deriesgos. Documento con el plan de tratamiento de riesgos. Documentos revisados yaprobados por la Alta Dirección.	Guía No 7 - Gestión de Riesgos. Guía No 8 Controles de Seguridad.
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan decomunicación, sensibilización y capacitación
Plan de diagnóstico de IPv4 aIPv6.	Documento con el Plan de diagnóstico para la transicióndе IPv4 a IPv6.	Guía No 20 - TransiciónIPv4 a IPv6.

A continuación, se explica de manera general los productos de la fase de planificación del Modelo de Seguridad y Privacidad de la Información:

a. **Política de seguridad y privacidad de la información**: La Política de Seguridad y Privacidad de la información estará 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 contendrá 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.

- ✓ 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 explica 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.

b. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA DE INFORMACIÓN.

Mediante la política de Escritorio y Pantalla limpia, el proceso permite definir reglas que evitaran el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos.

c. Procedimientos de Seguridad de la Información: 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, se tomará como referencia la Guía No 3 - describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la entidad.

d. Roles y Responsabilidades de Seguridad y Privacidad de la Información: La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad. Para desarrollar estas actividades, se tomará como referencia la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.

e. Inventario de activos de información: La entidad desarrollará la metodología de gestión de activos de la Guía No.5, que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

f. Integración del MSPI con el Sistema de Gestión documental: La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación. Para tal efecto tomará como referencia La Guía No 6 - Gestión Documental, la cual brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente.

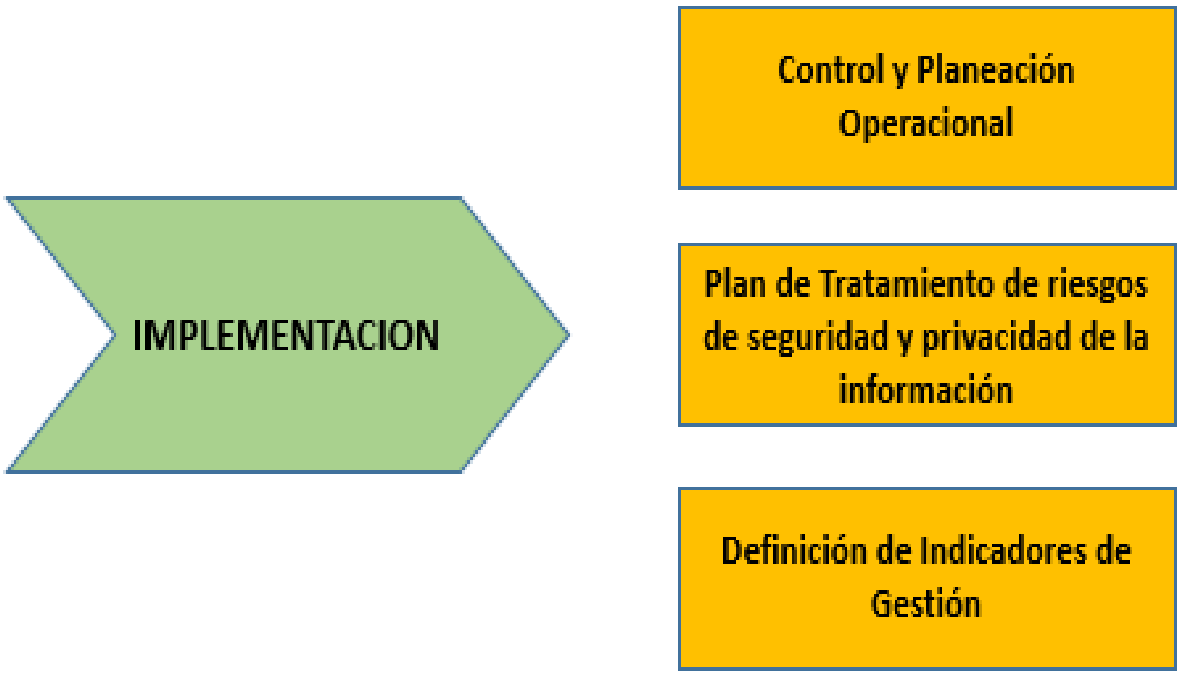
g. Identificación, Valoración Y Tratamiento de Riesgos: La entidad aplicará la metodología de gestión del riesgo de seguridad digital, según los lineamientos del DAFP y la Guía No 8 - Controles de Seguridad.

h. **Plan de Comunicaciones:** La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad. Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad. Para estructurar se tomará como referencia la Guía No 14 – plan de comunicación, sensibilización y capacitación.

i. **Plan de transición de IPv4 a IPv6:** Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia, que indica las actividades específicas a desarrollar.

3.3 Implementación

En esta fase la Entidad llevará a cabo las actividades de la fase de planeación.



Fases de Implementación

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

Implementación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Planificación y Control Operacional.	Documento con la estrategia de Planificación y control operacional revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Implementación Política escritorio y pantalla Limpia.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09LI.INF.10 LI.INF.11LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por eldueño de cada proceso.	Documento con ladeclaración de aplicabilidad. Documento con el plande tratamiento de riesgos.	
Indicadores DeGestión.	Documento conla descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadoresde Gestión SI.	
Plan de Transición deIPv4 a IPv6	Documento con lasestrategias del plande implementación de IPv6 en la entidad, aprobado por el área de TI	Documento con el Plande diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	LI.ST.13 LI.UA.01

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

a. Planificación y Control Operacional.

La entidad debe planificar, implementar y controlar los procesos y políticas necesarias 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.

La entidad 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.

b. Implementación del plan de tratamiento de riesgos.

Se debe implementar el plan de tratamiento de riesgos de seguridad digital, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía de Administración del Riesgo que emita el DAFP.

c. Indicadores De Gestión.

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

Los indicadores buscan medir:

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

d. Plan de Transición de IPv4 a IPv6.

Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad.

3.4 Evaluación de Desempeño

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

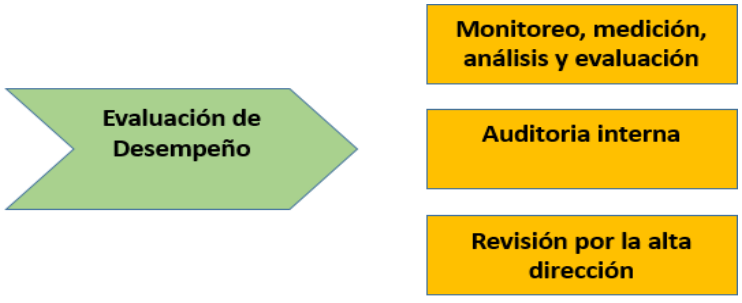


Tabla 4 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño.

Implementación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Plan de revisión y seguimiento, a la implementación delMSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16 – Evaluación del desempeño.	LI.ES.12,LI.ES.13 LI.GO.03,LI.GO.11 LI.GO.12,LI.INF.09 LI.INF.11 ,I.INF.13 LI.INF.14,LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08
Plan de Ejecuciónde Auditorias	Documento con elplan de ejecuciónde auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 15 – Guía de Auditoría.	

Plan de revisión y seguimiento a la implementación del MSPI.

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

- ✓ Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- ✓ Verificación de cumplimiento de Políticas propias del proceso.
- ✓ 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 permitirá la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

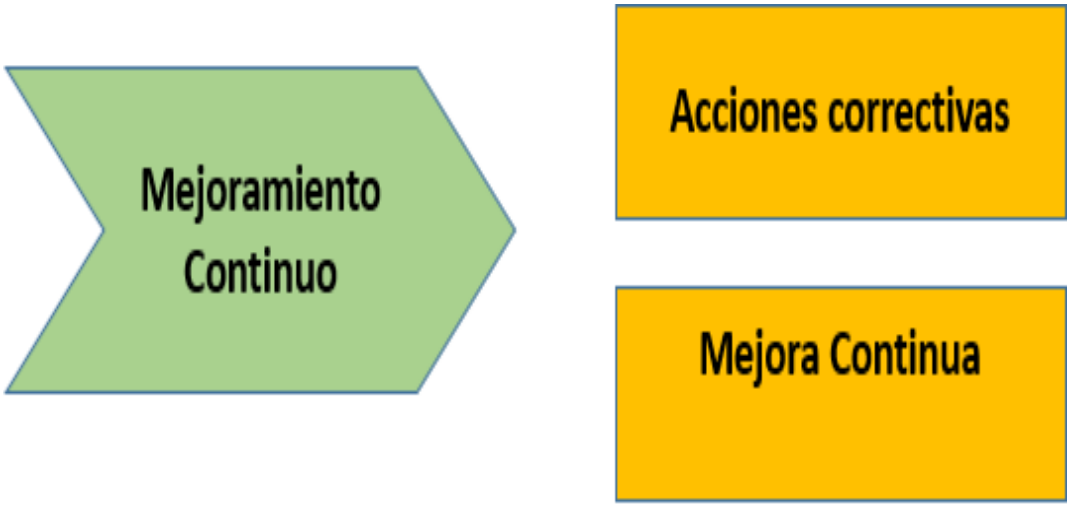
Plan de Ejecución de Auditorias

La entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Este plan estará a cargo del proceso de Requerimientos Tecnológicos.

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.

3.5 Mejora Continua

En esta fase la Entidad se consolida los resultados obtenidos de la fase de evaluación de desempeño, y se diseña el plan de mejoramiento continuo, tomando las acciones oportunas para mitigar las debilidades identificadas.



Fases Mejoramiento Continuo

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

Implementación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Plan de MejoraContinua	Documento con el plande mejoramiento. Documento con el plande comunicación de resultados.	Resultados de la ejecución del plan de Revisión y Seguimiento, a la implementación del MSPI Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI Guía 17 Mejora Continua	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10

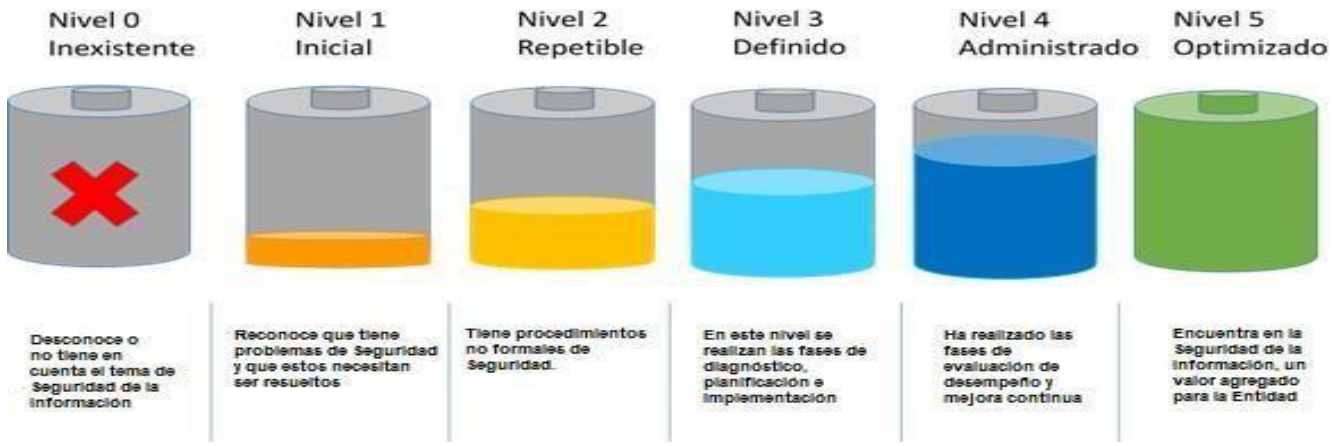
En esta fase la Entidad define y ejecuta el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

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

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

3.6 Modelo De Madurez

Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran la Entidad, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado. Es decir, se aplica en la fase de Diagnóstico y como herramienta de evaluación de los avances de la implementación del modelo



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 la Entidad.

Tabla 6 – Características de los Niveles de Madurez

Nivel	Descripción
Inexistente	✓ Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad. ✓ No se reconoce la información como un activo importante para su misión y objetivosestratégicos. ✓ No se tiene conciencia de la importancia de la seguridad de la información enla entidad.
Inicial	✓ Se han identificado las debilidades en la seguridad de la información. ✓ Los incidentes de seguridad de la información se traen de forma reactiva. ✓ Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos queden 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 lainformación. ✓ 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 dela seguridad de la información. ✓ La Entidad ha determinado los objetivos, alcance y límites de la seguridad de lainformación. ✓ La Entidad ha establecido formalmente políticas de Seguridad de la información yestas han sido divulgadas. ✓ La Entidad tiene procedimientos formales de seguridad dela Información ✓ La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de lainformación. ✓ La Entidad ha realizado un inventario de activos de información aplicando unametodología. ✓ 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 yprivacidad 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 un valoragregado 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 losobjetivos misionales. ✓ La entidad genera tráfico en IPv6.

3.7. Privacidad De La Información

Para cumplir con el objetivo del modelo de seguridad y privacidad de la información relacionado con garantizar el adecuado manejo de la información en poder de la entidad, la cual es uno de los activos más valiosos para la toma de decisiones, el MSPI propende por un doble enfoque, el del nivel de seguridad y el de privacidad de la información

A nivel de seguridad marca el derrotero para que se construyan políticas de seguridad a fin de salvaguardar la misma a nivel físico y lógico, de manera que se garantice su integridad, disponibilidad y autenticidad.

El nivel de seguridad se complementa con el nivel de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o a 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.

Es necesario 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 PQRSDF
- ✓ La Transferencia de información a terceros (otras entidades o países).

Se debe tener en cuenta los siguientes temas.

3.8. 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.

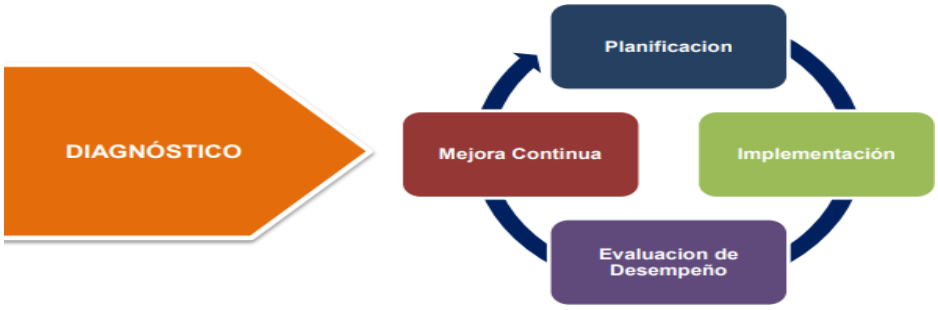
Identificar los riesgos de privacidad

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 y el impacto que puede generar su causación.

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.



Diagnóstico

En esta fase se identifica 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 utiliza 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 la Entidad para otorgar un nivel adecuado de protección a esta información.

Diagnóstico			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Diagnostico	Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad. Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	
	Documento con el resultado del diagnóstico realizado por la entidadcon la clasificación y distinción de los activos de información teniendoen 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.

Planificación

En esta segunda etapa se traza 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.

Planificación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Planificación	Documento con la política de privacidad, debidamente aprobada por la alta dirección y socializada alinterior de la entidad. Manual de políticas de seguridad yprivacidad de la información, aprobada por la alta dirección y socializada al interior de la entidad. Verificación del funcionamiento adecuado de la política Escritorio y pantalla Limpia. Documento con el plan de gestión dela privacidad sobre la información, aprobado por la alta dirección de la entidad. Definición de roles en relación conla Información. Procedimientos de privacidad. Plan de capacitación al interior de laentidad	Herramienta de diagnóstico. Guía No 4 - Roles y Responsabilidades de Seguridad y Privacidad de laInformación.	

Implementación

En esta fase se ejecutan las acciones trazadas en la etapa previa de planeación de manera que se diseñe un modelo de privacidad que permita cumplir con los mínimos legales y generar una política privacidad que 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.

Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Implementación	Documento con los riesgos contrala privacidad identificados y las medidas de solución adoptadas apartir 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 procedimientosajustados	Herramienta de Diagnóstico. Guía No 7 – Gestión de Riesgos.	

Fase de Evaluación del desempeño

Una vez implementadas las anteriores actividades el modelo de seguridad y 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.

Evaluación de Desempeño			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
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.	✓ Guía No 16 - Evaluación del Desempeño. ✓ Guía No 15 – Auditoria. Guía No 14 – Plan de Comunicación, sensibilización y capacitación.	

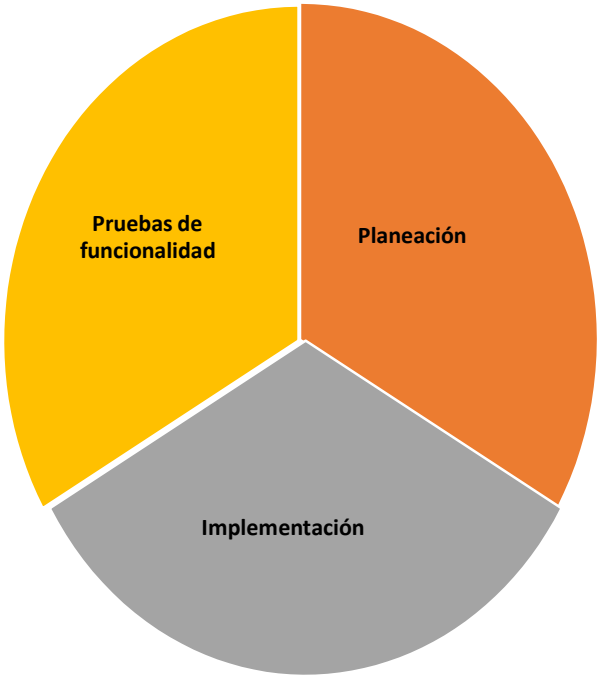
Mejora Continua

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.

Mejora Continua			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Mejora Continua	Documento con los resultados delplan de seguimiento Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de GestiónInstitucional o el que haga sus veces. Documento con el consolidado de las auditorias.	Guía No 16 – Evaluación delDesempeño. Guía No 17 - Mejora Continua.	

ADOPCIÓN DEL PROTOCOLO IPv6

A continuación, se mencionan las fases a cumplir para la transición del protocolo IPv4 a IPv6.



Planeación

Se define 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.

En la Tabla No 11 se describen las metas, entregables e instrumentos para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6.

Planeación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan y estrategia de transición deIPv4 a IPv6.	Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad 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 de para la implementación y aseguramiento del protocolo IPv6 en concordancia con la política de seguridad de las entidades.	Guía No 20 – Transición IPv4 aIPv6. Guía No 19 – Aseguramientodel protocolo IPv6. Circular 002 de 2011 delMinTIC.	

Implementación

Actividades de 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 de las entidades, entre otras.

En la Tabla No 12 se describen las metas, entregables e instrumentos para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia.

Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Implementación del plan y estrategia detransición de IPv4 aIPv6.	Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la altaDirección.	✓ Guía No 20 – Guía Transición de IPv4 a IPv6 para Colombia. ✓ Guía No 19 Guía de Aseguramiento del ProtocoloIPv6.	

Pruebas de Funcionalidad

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. Así mismo se elabora un inventario final de servicios y sistemas de comunicaciones, bajo el nuevo esquema de funcionamiento de IPv6

Pruebas de Funcionalidad			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Plan de Pruebas de funcionalidad IPV4 alPV6	Documento con los cambios detallados de lasconfiguraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de implementación Acta de cumplimiento a satisfacción de la Entidadcon respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos en la implementación Documento de inventario final de la Infraestructura TI sobre el protocolo IPV6	✓ Guía 20 – Guía transición de IPV4 a IPV6 para Colombia ✓ Guia 19 - Guía de Aseguramiento delprotocolo IPV6.	

ELABORÓ	REVISÓ	APROBÓ
FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL
PROFESIONAL UNIVERSITARIO REQ.TECNOLOGICOS	**PROFESIONAL UNIVERSITARIO PLANEACION**	**GERENTE**

CONTROL DE CAMBIOS			
FECHA	DESCRIPCION DEL CAMBIO	VERSION	MODIFICADO POR
10/04/2021	Aprobado por Comité Institucional de Gestión y Desempeño.	V1	Profesional Universitario de Requerimientos Tecnológicos.
22/02/2022	Aprobado por Comité Institucional de Gestión y Desempeño.	V2	Profesional Universitario de Requerimientos Tecnológicos.
30/01/2023	Aprobado por Comité Institucional de Gestión y Desempeño.	V3	Profesional Universitario de Requerimientos Tecnológicos.