GRUPO INTERNO DE SERVICIOS TECNOLÓGICOS.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

2025.

tabla de contenido

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

1. INTRODUCCION.

Las Universidad del Magdalena. ha establecido una política clara de apoyo y compromiso con la Seguridad de la Información.

En materia de Gobierno Digital, Colombia cuenta con una política de estado que ha venido evolucionando permanentemente en su alcance e implementación, reconociendo el uso de las Tecnologías de la Información y las Comunicaciones -TIC, como un instrumento fundamental para mejorar la gestión pública y la relación del Estado con los ciudadanos. En este sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC, es consecuente con la realidad de que las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Razón por la cual el ministerio como entidad encargada de diseñar, adoptar y promover políticas, planes, programas y proyectos en el uso y apropiación de las TIC, establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las Entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente Y efectiva los activos de información, infraestructura crítica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

Teniendo en cuenta lo anterior, la Universidad del magdalena mediante este documento adopta el Modelo de Seguridad y Privacidad de la Información – MSPI elaborado por Min TIC, el cual define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de la Unimag

El sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases, las cuales permitirán a la Universidad del magdalena, gestionar y

mantener adecuadamente la seguridad y privacidad de sus activos de información:

1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la UNIVERSIDAD DEL MAGDALENA en la adopción del MSPI, su resultado será un insumo para la fase de planificación y luego al finalizar la fase 4 de mejora continua.

2. Planificación: En esta parte, la UNIVERSIDAD DEL MAGDALENA determina las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

3. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

4. Evaluación de desempeño: Determina el sistema y forma de evaluación de la adopción del modelo.

5. Mejoramiento Continuo: Establece procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

Si bien es cierto, de acuerdo a la normativa vigente las entidades del estado deben trabajar bajo un nuevo concepto de Gobierno Digital, la universidad del magdalena ha venido trabajando en la implementación del Sistema de Seguridad de la Información SGSI, a partir de la DECLARACIÓN DE APLICABILIDAD DEL SGS, donde se incluyen todos los controles del Anexo A, vinculado a la norma internacional ISO/IEC 27001

2. AUDIENCIA.

El presente documentos está dirigido a los servidores, contratistas y tercerizados y partes interesadas en cumplimiento de lo establecido en el artículo 2.2.9.1.1.2 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

ARTÍCULO 2.2.9.1.1.2. *Ámbito de aplicación.* Los sujetos obligados a las disposiciones contenidas en el presente capítulo serán las entidades que conforman la administración pública en los términos del Artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas.

PARÁGRAFO. La implementación de la Política de Gobierno Digital en las ramas legislativa y judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los Artículos 113 y 209 de la Constitución Política.

3. DEFINICIONES

El Modelo incluye la siguiente terminología para su comprensión:

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso 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 ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- Activos de Información y recursos: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).
- 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 dicho riesgo. (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: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- 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 (Ley1712 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).
- 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.
- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimizarían o cifrado.
- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000) y según Norma NTC-ISO 22301 del 20 de noviembre de 2019, Seguridad y resiliencia. Sistema de gestión de continuidad del negocio. Requisitos. Se define en el numeral 3.4 como: Información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad del negocio.
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).
- Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad

4. MARCO JURIDICO Y NORMATIVO

La Universidad del Magdalena. Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC, se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la Secretaría Distrital de Planeación:

Constitución Política de Colombia. Artículos 15, 209 y 269.

Ley 1581 de 201: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014: Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1083 de 2015: " Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de.

"11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

CONPES 3854 de 2016: Política Nacional de Seguridad digital.

Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Decreto 2106 de 2019: establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario.

Resolución 500 de 2021: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

5. ALCANCE DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL MAGDALENA

El Modelo de Seguridad y Privacidad de la Información – MSPI, se constituye en el instrumento que soportará la Seguridad de la Información en la Universidad del Magdalena - Unimag, que según el Manual de Gobierno Digital busca "que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información - MSPI, que contempla 6 niveles de madurez"; los niveles de madurez han sido determinados en la etapa previa a la actualización del presente documento a partir de la herramienta de diligenciamiento del instrumento de medición del MSPI de Min TIC, cuya metodología describe los niveles de evaluación aplicados a la seguridad de la información en el instrumento:

- Inexistente

- Inicial
- Repetible
- Efectivo
- Gestionado y;
- optimizado

Las fases del Modelo de Seguridad y Privacidad de la Información - MSPI y los resultados como producto del desarrollo de la fase de DIAGNÓSTICO son la base para la definición del Plan de Implementación del MSPI que cubrirá las fases de PLANIFICACIÓN, OPERACIÓN, EVALUACIÓN DEL DESEMPEÑO Y MEJORA CONTINUA, como ciclo de operación definido en por el Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC para el Modelo.

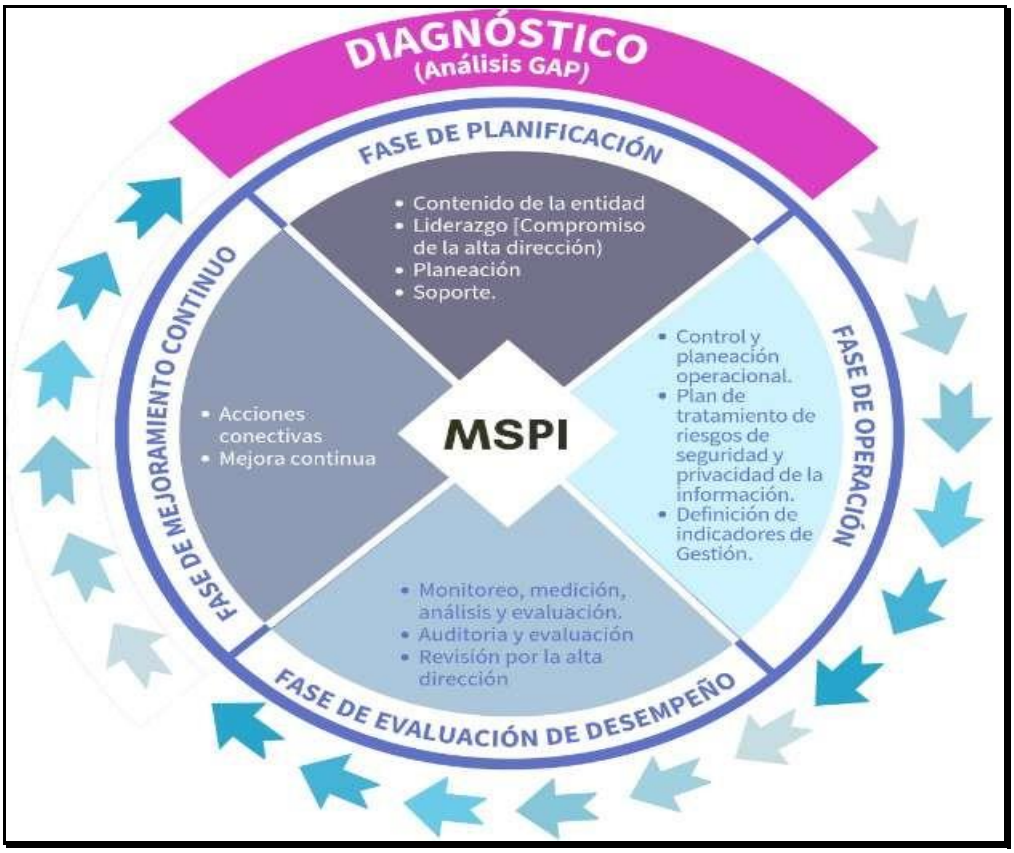

Figura 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información
Fuente: "Modelo de Seguridad y Privacidad de la Información" - Anexo 1 de la Resolución 500 de 2021 de Min TIC.

A continuación, se describen las fases del modelo que dan cumplimiento a las directrices del Gobierno Nacional (Resolución 500 de 2021 de 2021, Anexo 1 Modelo

de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones dispuesto por Min Tic) y Gobierno Territorial (Alta Consejería Distrital de Tecnologías de Información y Comunicaciones).

El plan de acción por fases que se presenta en los siguientes títulos se elabora con base en la Tabla de Escala utilizada por MIN TIC en la herramienta de autodiagnóstico que se encuentra alineada con la metodología del Modelo de Seguridad y Privacidad de la Información.

Tabla 1. Escala de Valoración de Controles
ISO 27001:2013 ANEXO A

Descripción	Calificación	Criterio
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

6. FASE DE DIAGNÓSTICO

La fase de diagnóstico permite a la Unimag establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realiza un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación.

Se debe realiza antes de iniciar la fase de planificación, y actualizarlo posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño será incluido como un insumo, en la fase de mejoramiento continuo.

Objetivo

Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la Entidad, como punto de partida para la implementación del MSPI.

Lineamiento:

Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la Entidad respecto a la seguridad y privacidad de la Información.

DIAGNÓSTICO	
Entrada	**Salida**
• Para la identificación del estado de implementación del MSPI, se debe utilizar la herramienta de autodiagnóstico del MSPI. • Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.	• Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la Entidad, y sus acciones de mejora.

7. FASE 1 PLANIFICACIÓN

En el desarrollo de esta fase se debe utilizar los resultados de la fase anterior con el objetivo de proceder a elaborar el Plan de Seguridad y Privacidad de la Información para cada una de las vigencias el cual incluye la planeación del tiempo y recursos.

Los documentos que se deben generar en esta fase son:

- Alcance MSPI
- Acto administrativo con las funciones de seguridad y privacidad de la información.
- Política de seguridad y privacidad de la información
- Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información
- Procedimiento de inventario y Clasificación de la Información e infraestructura crítica
- Metodología de inventario y clasificación de la información e infraestructura crítica
- Procedimiento de gestión de riesgos de seguridad de la información
- Plan de tratamiento de riesgos de seguridad de la información
- Declaración de aplicabilidad
- Políticas de Seguridad de la Información

Plan de capacitación, sensibilización y comunicación de seguridad de la información

7.1 CONTEXTO

7.1.1 Comprensión de la organización y de su contexto

Objetivo:

Conocer en detalle las características de la Entidad y su entorno, que permitan implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada Entidad.

Lineamiento:

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

Determinar los elementos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la Entidad.

FASE 1 PLANIFICACIÓN 7.1.1 Comprensión de la organización y de su contexto	
Entradas	**Salidas**
• Para establecer el contexto de la Entidad debe tener en cuenta los aspectos relacionados en el Manual Operativo MIPG. • Modelo estratégico, modelo de procesos, modelo de servicios y modelo organizacional siguiendo el Marco de Referencia de Arquitectura Empresarial definido por Min TIC. • Plan estratégico de la Entidad	Documentos obligatorios: Contexto de la entidad (Política de Planeación Institucional).

7.1.2 Necesidades y expectativas de los interesados

Objetivo:

Conocer las expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información, para asegurar que el modelo garantizará su cumplimiento.

Lineamiento:

Se debe determinar partes interesadas internas o externas como las personas, entidades u organizaciones que pueden influir directamente en la seguridad y

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

privacidad de la información de la Universidad del Magdalena o que pueden verse afectados en caso de que estas se vean comprometidas. Adicionalmente, se determinan sus necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información. Los requisitos de las parte interesadas deberán incluir los requisitos legales, reglamentarios y contractuales

FASE 1 PLANIFICACIÓN 7.1.2 Necesidades y expectativas de los interesados	
Entrada	**Salidas**
• 7.1.1 Comprensión de la organización y de su contexto. • Política de Planeación institucional (7.1.1Comprensión de la organización y de su contexto). • Plan Nacional de Desarrollo. • Política de Gobierno Digital. • Entrevistas con los líderes de procesos de la Entidad. • Listado de entidades de orden nacional o territorial que se relacionan directamente el cumplimiento misional de la Entidad. • Listado de proveedores de la Entidad. • Listado de operadores de la Entidad. • Normatividad que le aplique a la Entidad de acuerdo con funcionalidad	Documentos obligatorios: Partes interesadas. (Política de Planeación Institucional).

7.1.3 Definición del alcance del MSPI

Objetivo:

Identificar qué información (generada o utilizada en los procesos de la Entidad) será protegida mediante la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI.

Lineamiento:

Determinando los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la Entidad, estableciendo a qué procesos y recursos tecnológicos se realizará la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, teniendo en cuenta los requisitos de las partes interesadas incluyen los requisitos legales, reglamentarios y contractuales.

FASE 1 PLANIFICACIÓN 7.1.3 Definición del alcance del MSPI	
Entradas	**Salidas**
• 7.1.1 Comprensión de la organización y de su contexto. • 7.1.2 Necesidades y expectativas de los interesados. • Modelo de procesos, modelo organizacional, modelo de servicios y catálogo de servicios tecnológicos; siguiendo el Marco de Referencia de Arquitectura Empresarial definido por Min TIC. • Presupuesto disponible para implementar el MSPI. • Listado de las sedes físicas donde opera la Entidad.	• Alcance del MSPI, (Este alcance puede estar integrado al Manual del Sistema de Gestión, o en el documento del Modelo de Planeación y Gestión).

7.2 LIDERAZGO

7.2.1 Liderazgo y Compromiso

Objetivo:

Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño para conseguir los objetivos definidos para la implementación del MSPI.

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

Lineamiento:

Como sujeto obligado debe incluir dentro del comité institucional de gestión y desempeño o quien haga sus veces, las funciones relacionadas con seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, por medio de un acto administrativo. Con el propósito de garantizar el éxito de su implementación, que permita dar cumplimento entre otras, a las siguientes acciones

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la Entidad,
- Comunicar en la Entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI.

FASE 1 PLANIFICACIÓN 7.2.1 Liderazgo y Compromiso	
Entradas	Salidas
• 7.1.3 Definición del alcance del MSPI. • Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por Min TIC. • Necesidades y expectativas de los interesados.	• Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.

7.2.2 Política de seguridad y privacidad de la información.

Objetivo:

Orientar y apoyar por parte de la alta dirección de la Secretaría Distrital de Planeación a través del comité de gestión y desempeño la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación vigente.

Lineamiento:

Se debe establecer en la política de seguridad y privacidad de la información el enfoque de la entidad, para ello debe tener en cuenta:

- Misión de la Entidad
- Normatividad vigente con la cual se debe contar para el funcionamiento de la Entidad
- Establecer compromiso del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua una vez el MSPI sea adoptado
- Estar alineada con el contexto de la Entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información.
- Se deben asignar los roles y responsabilidades que se identifiquen.
- Ser incluidos y aprobados los temas de seguridad de la información y seguridad digital en el comité de gestión y desempeño institucional, modificando el acto administrativo de conformación de este, aprobado por el mismo comité y expedido por el nominador o máxima autoridad de la Entidad.
- Ser comunicada al interior de la Entidad y a los interesados que aplique. La política establece la base respecto al comportamiento de personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la Entidad.

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

FASE 1 PLANIFICACIÓN 7.2.2 Política de seguridad y privacidad de la información	
Entradas	**Salidas**
• Comprensión de la organización y de sucontexto. • Necesidades y expectativas de los interesados. • Definición del alcance del MSPI. • Requerimientos normativos.	• Acto administrativo con la adopción de la Política de seguridad y privacidad de la información.

7.2.3 Roles y responsabilidades

Objetivo:

Asegurar que los funcionarios de la Entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.

Lineamiento:

Articular con las áreas o dependencias de la Entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño, para que sean aprobados y comunicados dentro de la Entidad. Se debe delegar a un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI; si el cargo no existe en la Entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz.

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

FASE 1 PLANIFICACION 7.2.3 Roles y responsabilidades	
Entrada	Salidas
• 7.1.3 Definición del alcance del MSPI • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por Min TIC.	Roles y responsabilidades

7.3 PLANIFICACIÓN

7.3.1 Identificación de activos de información e infraestructura critica

Objetivo:

Estructurar una metodología que permita identificar y clasificar los activos de información

Lineamiento:

Las Universidad del Magdalena debe definir y aplicar un proceso de identificación y clasificación de la información, que permita:

- Determinar o identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.
- Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.
- Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso.

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

PLANIFICACIÓN 7.3.1 Identificación de activos de información e infraestructura crítica	
Entradas	**Salidas**
• 7.1.3 Definición del alcance del MSPI. • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por Min TIC. • Guía para la Gestión y Clasificación de Activos de Información.	• Procedimiento de inventario y clasificación de la información. • Documento metodológico de inventario y clasificación de la información.

7.3.2 Valoración de los riesgos de seguridad de la información

Objetivo:

Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información.

Lineamiento:

Las Universidad del Magdalena debe definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita:

- Identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la Entidad dentro del alcance del MSPI. Identificar los dueños de los riesgos.
- Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.
- Determinar el apetito de riesgos definido por la Entidad
- Establecer criterios de aceptación de los riesgos.
- Aplicar el proceso de valoración del riesgo que permita determinar los

riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance. Determinar los niveles de riesgo.

- Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral.

Priorización de los riesgos analizados para su tratamiento. Se debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables.

FASE 1: PLANIFICACIÓN 7.3.2 Valoración de los riesgos de seguridad de la información	
Entrada	**Salidas**
• 7.1.3 Definición del alcance del MSPI. • 7.2.2 Política de seguridad y privacidad de la información. • Directorio de servicios de componentes de información, de acuerdo con el Marco de Referencia de Arquitectura Empresarial definido por Min TIC. • Inventario de activos de información de la Entidad usando el proceso de valoración de riesgos de la seguridad de la información definido por medio de: Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía	• Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno.

7.3.3 Plan de tratamiento de los riesgos de seguridad de la información

Objetivo:

Estructurar una metodología que permita definir las acciones que debe seguir

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

la Entidad para poder gestionar los riesgos de seguridad y privacidad de la información.

Lineamiento:

La Entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:

- Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
- Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.
- Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad.
- Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

FASE 1: PLANIFICACIÓN 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información	
Entradas	Salidas
• Inventario de activos de información de la Entidad. • 7.3.2 Valoración de los riesgos de seguridad de la información	• Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). • Declaración de aplicabilidad, aceptada y aprobadas en el comité de gestión institucional.

7.4 SOPORTE

7.4.1 Recursos

Objetivo:

La entidad debe contar con los recursos necesarios para la implementación del MSPI

Lineamiento:

La Entidad debe determinar y proporcionar los recursos necesarios para adoptar el MSPI, teniendo en cuenta que es un proceso transversal de la Entidad, se requiere que se disponga de los recursos financieros, humanos (dedicación de horas/hombre) de sus colaboradores y en general cualquier recurso que permita la adopción, implementación, mantenimiento y mejora continua del MSPI.

Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI.

FASE 1: PLANIFICACIÓN 7.4.1 Recursos	
Entrada	**Salidas**
• 7.1 Contexto. • 7.1.3 Definición del alcance del MSPI. • 7.2.2 Política de seguridad y privacidad de la información. • 7.2.3 Roles y responsabilidades. • 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.	• Incluir dentro de los proyectos de inversión de la Entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido.

Lineamiento:

La Entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para:

- Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del MSPI.

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

- Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.
- Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información.
- Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.

FASE 1: PLANIFICACIÓN 7.4.2 Competencia, toma de conciencia y comunicación	
Entrada	**Salidas**
• 7.1.3 Definición del alcance del MSPI. • 7.2.3 Roles y responsabilidades. • Manual de funciones de la Entidad. • Plan de capacitación Institucional.	• Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones – PIC. • Plan de comunicaciones del modelo de seguridad.

8. FASE 2 OPERACIÓN

Una vez culminada las actividades del MSPI de la fase de 7.3 Planificación, se llevará acabo la implementación de los controles, con el fin de dar cumplimiento con los requisitos del MSPI. Los documentos que se deben generar en esta fase son:

- ❖ Plan de implementación de controles de seguridad y privacidad de la información.
- ❖ Evidencia de la implementación de los controles de seguridad y privacidad de la información.

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

8.1 Planificación e implementación

Objetivo:

Implementar los planes y controles para lograr los objetivos del MSPI.

Lineamiento:

La Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional de gestión y desempeño.

FASE 2: OPERACIÓN 8.1 Planificación e implementación	
Entrada	**Salidas**
• 7.3.2 Valoración de los riesgos de seguridad de la información. • Plan de 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.	• Plan de implementación de controles deseguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. • Evidencia de la implementación de los controles de seguridad y privacidad de la información.

9. FASE 3 EVALUACIÓN Y DESEMPEÑO

Una vez culminada las actividades del MSPI, se evalúa 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, MIPG y los requerimientos de la Ley 1581 de 2012 "Protección de datos personales", Ley 1712 de 2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

9.1 Seguimiento, medición, análisis y evaluación

Objetivo:

Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.

Lineamiento:

La Universidad del Magdalena debe conocer de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

FASE 3: EVALUACIÓN Y DESEMPEÑO 9.1 Seguimiento, medición, análisis y evaluación	
Entrada	**Salidas**
➢ Documento con los resultados de la valoración de los riesgos. ➢ Documento con los resultados del tratamiento de riesgos de seguridad de la información. ➢ Resultado de la implementación de los controles.	➢ Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018. ➢ Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.

9.2 Auditoría Interna

Objetivo:

Realizar seguimiento a la implementación del MSPI

Lineamiento:

Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del MSPI.

FASE 3: EVALUACIÓN Y DESEMPEÑO 9.2 Auditoría Interna	
Entrada	Salidas
• Todos los documentos producto de las salidas de las fases anteriores del MSPI. • El informe de los resultados de las evaluaciones independientes, seguimientos y auditorías. • Informes y compromisos adquiridos en los comités institucionales de gestión y desempeño. • El informe de los incidentes de seguridad y privacidad de la información reportada y la solución de estos. • Informe sobre los cambios PESTEL (legales, procesos, reglamentarios, regulatorios, tecnológicos, ambientales, o aquellos en el marco del contexto de la organización) en la Entidad. • Indicadores definidos y aprobados para la evaluación del MSPI.	• Resultados de las auditorías internas. • No conformidades de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno.

9.3 Revisión por la Dirección

Objetivo:

Revisar el MSPI de la Entidad, por parte de la alta dirección (comité institucional de gestión y desempeño), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

Lineamiento:

Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño, o cuando el nominador lo determine.

FASE 3: EVALUACIÓN Y DESEMPEÑO 9.3 Revisión por la Dirección	
Entrada	Salidas
• Todos los documentos del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la Entidad.	• Revisión a la implementación. • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.

10. FASE 4 MEJORAMIENTO CONTINUO

Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

10.1 Mejora

Objetivo:

Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

Lineamiento:

La Secretaría Distrital de Planeación debe elaborar un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI.

FASE 4: MEJORAMIENTO CONTINUO 10.1 Mejora	
Entrada	**Salidas**
• Resultados de la ejecución del plan deseguimiento, evaluación y análisis para el MSPI. • Resultados de auditorías y revisiones independientes al MSPI.	• Plan anual de mejora del MSPI

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

11. DEFINICIÓN DE INDICADORES MSPI

Tabla 2. Indicadores de Gestión Seguridad de la Información						
PRODUCTO	NOMBRE DEL INDICADOR	OBJETIVO DEL INDICADOR	FÓRMULA	TIPO	UNIDAD DE MEDIDA	META PERIODO
ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	Nivel de Compromiso	Hacer seguimiento, al compromiso sobre el sistema seguridad de la información	# de revisiones realizadas por la alta dirección al año / # revisiones programadas para el año	Eficacia	Porcentaje	100%
CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN	Activos de Información de la Unimag revisados y actualizados	Revisar y actualizar los activos de información de la Unimag por proceso	# de procesos con activos de información (RAI) revisados y actualizados en la vigencia/# de procesos de la Unimag	Eficacia	Porcentaje	95%
PLAN DE SENSIBILIZACIÓN Y COMUNICACIÓN	Nivel de Ejecución del Plan de Sensibilización y Comunicación en Seguridad de la Información de la Unimag	Hacer seguimiento a la ejecución del Plan de Sensibilización y Comunicación en Seguridad de la Información de la Unimag	# de estrategias desarrolladas al año que cumplen con la meta de ejecución >=80% / # de estrategias programadas para desarrollar al año siguiendo lo establecido en el plan de sensibilización	Eficacia	Porcentaje	80%

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Porcentaje de políticas de Seguridad de la Información actualizadas o definidas en la vigencia	Mide el porcentaje de actualización o creación de políticas de seguridad de la información definida en la vigencia	# de políticas de Seguridad de la Información actualizadas o creadas en la vigencia / # de políticas de seguridad de la información planeada para actualización o creación en la vigencia	Eficacia	Porcentaje	90%
EJECUCIÓN DEL MPSI	Nivel de Madurez de las fases del MPSI	Controlar el avance de las Fases del MSPI en términos de Madurez	# de actividades desarrolladas durante la vigencia en el Plan de Acción del MPSI / # de actividades definidas para desarrollar en la vigencia	Eficacia	Porcentaje	90%
GESTIÓN DE INCIDENCIAS DE SEGURIDAD	Porcentaje de atención a las incidencias de seguridad realizadas por los usuarios de la Unimag	Medir el porcentaje de incidencias de Seguridad de la Información atendidas en la vigencia	(# de incidencias de seguridad atendidas en la vigencia /# de incidencias de seguridad recibidas en la vigencia) *100	Eficacia	Porcentaje	92%

12. ANEXOS DE CONSULTA

Hacen parte del presente documento los anexos definidos en el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones de febrero de 2021[1]:

- Controles y objetivos de control
- Guía - Roles y responsabilidades
- Guía - Gestión inventario clasificación de activos e infraestructura critica
- Guía para la gestión de riesgos de seguridad de la información (Anexo 4. DAFP)
- Guía - Indicadores Gestión de Seguridad de la Información

[1] Resolución 500 de 2021 de Min TIC. Anexo 1 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pd

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

13. DERECHOS DE AUTOR

Teniendo en cuenta que el documento es la adopción del Modelo de Seguridad y Privacidad de la Información definido por MITNIC, todas las referencias a los documentos son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones – MIN TIC.

En consecuencia, el Min TIC goza de los derechos de autor establecidos en la ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos del El Modelo de Gestión de Riesgos de Seguridad Digital - MGRSD y su contenido. Las reproducciones, referencias o enunciaciones de estos documentos deberán ir siempre acompañadas por el nombre o seudónimo del titular de los derechos de autor (Ministerio de Tecnologías de la Información y las Comunicaciones). Lo anterior, sin perjuicio de los derechos reservados por parte de entidades tales como la International Standard Organization (ISO), ICONTEC, entre otras, respecto de referencias, definiciones, documentos o contenido relacionado en el Modelo de Gestión de Riesgo de Seguridad Digital (MGRSD) y sus documentos o anexos que son de su autoría o propiedad.

Elaboró: Nombre – Ing. Edwin Navarro Orozco – Esp. Ciberseguridad.
Revisó: Nombre - Ing. Hildemar David Quintana Hernández. - *Jefe Oficina Grupo Interno de Servicios Tecnológicos.*

Carrera 32 No.22-08 Sector San Pedro Alejandrino
Bloque VIII, 1er Piso Santa Marta - Colombia
PBX: (57-5) 4381000 Ext. 8000 y 2188
grupotic@unimagdalena.edu.co
www.unimagdalena.edu.co

43