Educación

Somos la Revolución del Cambio

Plan Estratégico de Tecnologías de la Información - PETI

Ministerio de Educación Nacional de Colombia

Daniel Rojas Medellín

Ministro de Educación Nacional

Daniel Guillermo Torres Niño

Jefe Oficina de Tecnología y Sistemas de Información - OTSI

TABLA DE CONTENIDO

INTRODUCCIÓN

El Ministerio de Educación Nacional de acuerdo con lo indicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, en la Resolución 500 de 2021, 746 de 2022 y 02277 de 2025 que indica los lineamientos a seguir para dar cumplimiento a un MSPI (Modelo de Seguridad y Privacidad de la Información) efectivo:

"**ARTÍCULO 3. ADICIÓN DEL ARTÍCULO 6.1 A LA RESOLUCIÓN MINTIC NÚMERO 500 DE 2021**. Los sujetos obligados deben determinar e implementar los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo número 2 de la presente resolución, así como cumplir con los siguientes requerimientos y características.

1. Definir claramente los roles y responsabilidades de seguridad de la información con respecto a la relación con el proveedor.

2. Propender por mantener una arquitectura de seguridad al adquirir productos o servicios de Seguridad Digital.

3. Analizar los riesgos de Seguridad Digital propios de la integración de soluciones e implementar controles para su mitigación.

4. Implementar controles que permitan minimizar los riesgos asociados a la transferencia de datos generada por cambios de fabricante o proveedor.

5. Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación.

6. Optimizar la gestión de los riesgos de Seguridad Digital estableciendo estrategias soportadas en servicios de nube.

PARÁGRAFO. Los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo número 2, hacen parte integral de la presente resolución y serán actualizados por el MinTIC a través de las sucesivas versiones de cada uno de los documentos que lo componen y previo informe del equipo técnico. La actualización se publicará en la sede electrónica del MinTIC".

ARTÍCULO 4. Sistema de gestión de seguridad de la información y seguridad digital. Los sujetos obligados deben aplicar los modelos, guías y otros

documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones mediante el habilitador de seguridad y privacidad de la información dentro de la Política de Gobierno Digital y propenderán incorporando estándares internacionales y sus actualizaciones o modificaciones, así como otros marcos de trabajo que defina mejores prácticas en la materia.

ARTÍCULO 5. La estrategia de seguridad digital. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:

1. Ser aprobada mediante un acto administrativo general.
2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.
4. 4.Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces.
5. La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.

6. Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad digital.

Parágrafo 1. Los sujetos obligados deben adoptar el Modelo de Seguridad y Privacidad de la Información – **MSPI** señalado en el **Anexo 1** de la presente resolución, como habilitador de la política de Gobierno Digital.

ARTÍCULO 1. ACTUALIZACIÓN A LA RESOLUCIÓN MINTIC NÚMERO 500 DE 2021. Actualícese el Anexo 1 de la Resolución número 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"

Dicho lo anterior, se construye un plan de trabajo de mejora continua para fortalecer el modelo de seguridad y privacidad del Ministerio de Educación y generar confianza en el tratamiento de la información en los procesos de la entidad.

https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

https://www.mintic.gov.co/portal/715/articles-403045_recurso_1.pdf

OBJETIVO

Implementar un Plan integral de Seguridad y Privacidad de la Información que garantice la protección de los datos sensibles y el cumplimiento de las normativas vigentes, alineado con el Modelo de Seguridad y Privacidad de la Información y la norma internacional **ISO/IEC ISO 27001:2022.** Este plan debe promover la mejora continua de los procesos de seguridad, mitigar los riesgos asociados con el manejo de la información y asegurar la confidencialidad, integridad y disponibilidad de la información acorde a lo establecido en la ST-PO-01 Política General de Seguridad de la Información del Ministerio de Educación Nacional.

ALCANCE

El objetivo principal de este plan es fortalecer la seguridad digital en todos los procesos del Ministerio de Educación Nacional-MEN, abarcando todos los niveles funcionales y organizacionales. El enfoque está orientado a garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando que la información institucional maneja el Ministerio se encuentre protegida frente a amenazas y vulnerabilidades emergentes.

Este plan establecerá un marco robusto que permita la implementación de controles físicos y lógicos de seguridad y el desarrollo de protocolos de privacidad que salvaguarden los activos de información en toda la institución. A través de la adopción de buenas prácticas y el cumplimiento de normativas internacionales, como la **ISO/IEC 27002**, se impulsará una cultura de mejora continua en la gestión de riesgos digitales.

Al finalizar la ejecución de este plan, el Ministerio contará con procesos y procedimientos más maduros en términos de seguridad y privacidad de la información. Estos avances permitirán una mejor gestión de riesgos, un aumento en la resiliencia operativa, y la consolidación de un entorno tecnológico confiable y seguro para el cumplimiento de los objetivos institucionales.

DEFINICIONES

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).

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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 servicios de información que se encuentran interconectados.

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

Control: es cualquier medida, política, procedimiento o mecanismo implementado para **mitigar o gestionar los riesgos** dentro de niveles aceptables para la organización. Los controles abarcan tanto aspectos técnicos como organizativos, y se utilizan para **mantener el riesgo por debajo del nivel asumido**. También se conocen como **salvaguardas** o **contramedidas**. En términos simples, un control es una **acción que modifica el riesgo**, reduciendo su probabilidad o impacto.

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

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

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

Datos Personales Mixtos: para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

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

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 2157 de 2021.

Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

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).

NORMATIVIDAD Y METODOLOGÍA

El Ministerio de Educación ha desarrollado el modelo de seguridad y privacidad de la información de acuerdo con las siguientes resoluciones y políticas:

1. Resolución No. 017564 31 DIC 2019 en su Artículo 3. Modelos referenciales del Sistema Integrado de Gestión del Ministerio de Educación Nacional indica:

“Sistema de Gestión de Seguridad de la Información, recoge los lineamientos del Ministerio de las TIC para el desarrollo de la política de seguridad digital de MIPG, que busca gestionar adecuadamente la seguridad y privacidad de los activos de información, en el marco de la estrategia de «Gobierno Digital antes Gobierno en Línea» establecido en el Decreto 2573 del año 2014 y el Decreto 1078 de 2015”.

“Política SIG: El Ministerio de Educación Nacional se compromete a implementar y mejorar continuamente el SIG, articulando sus procesos entre sí y con las políticas de gestión y desempeño de MIPG, cumpliendo los requisitos de los modelos referenciales y demás normas que le sean aplicables y garantizando la calidad de los servicios que ofrece, a través de la gestión de los riesgos que puedan afectar el logro de sus objetivos institucionales, la protección del medio ambiente, la seguridad de la información y el bienestar integral de los colaboradores. Asimismo, se compromete con la escucha y análisis de las necesidades y expectativas de los grupos de valor, como parte de la evaluación periódica del cumplimiento y del desempeño del sistema, rindiendo cuentas sobre las decisiones tomadas para asegurar su conveniencia, adecuación, eficacia y alineación con las metas estratégicas de la entidad”

2. Resolución 004058 de 2024 Artículo 1. Adoptar las Políticas de Gestión y Desempeño Institucional. Adóptese como Políticas de Gestión y Desempeño Institucional las siguientes:

- Planeación Institucional.
- Gestión presupuestal y eficiencia del gasto público.
- Talento humano.
- Integridad.
- Transparencia, acceso a la información pública y lucha contra la corrupción.
- Fortalecimiento organizacional y simplificación de procesos.
- Servicio al ciudadano.

- Participación Ciudadana en la gestión pública.
- Simplificación, racionalización y estandarización de trámites, antes racionalización de trámites.
- Gestión documental.
- Gobierno Digital, antes gobierno en línea.
- Seguridad Digital.
- Defensa jurídica.
- Gestión de conocimiento y la innovación.
- Control interno.
- Seguimiento y evaluación de desempeño institucional.
- Mejora normativa
- Gestión de la información estadística
- Compras y contratación pública.

3. PO-01 Política General de Seguridad de la Información, donde se definen directrices, lineamientos, condiciones, pautas y establecimiento de controles necesarios para la protección de la información en el Ministerio de Educación Nacional-MEN, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

METODOLOGÍA

La metodología que se aplicará para este plan corresponde a lo que se conoce como el ciclo PHVA Planear, Hacer, Verificar y Actuar que en el nuevo modelo indicado por MinTIC corresponde a:

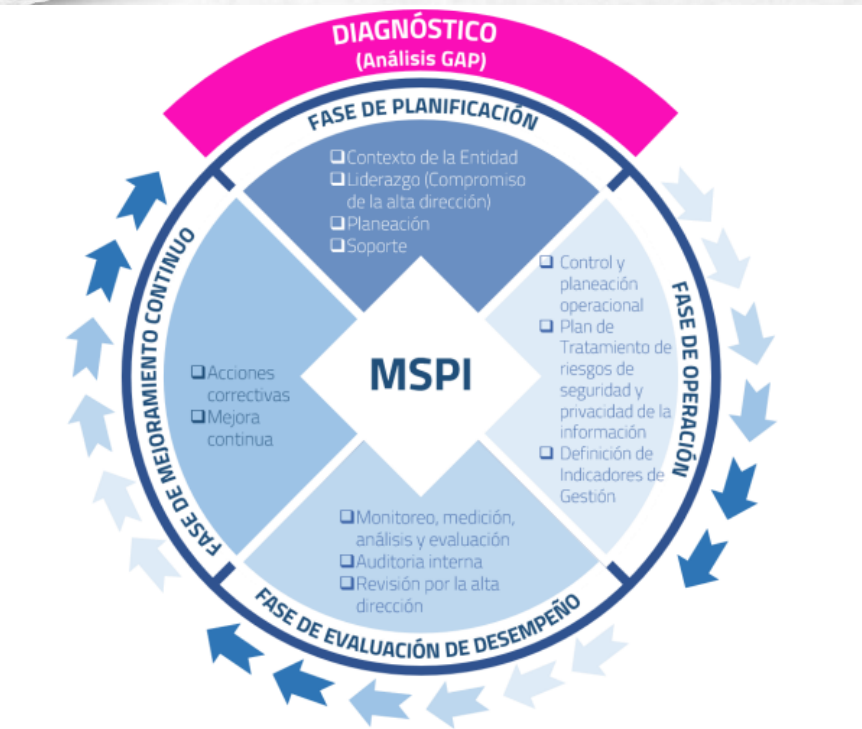

Ilustración Ciclo del Modelo de Seguridad y Privacidad de la Información (1)

“Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones”

Actualmente se cuenta con la documentación actualizada y formalizada dentro del SIG, de acuerdo a las acciones adelantadas en la vigencia anterior relacionada con la mejora continua del SGSI.

CUMPLIMIENTO DE LA IMPLEMENTACIÓN

Para asegurar el cumplimiento del plan de trabajo descrito en este documento, se llevará a cabo un seguimiento trimestral por parte de la subdirección de desarrollo organizacional SDO Este seguimiento permitirá verificar el avance de cada actividad programada, identificar posibles desviaciones y aplicar las acciones correctivas oportunas, asegurando que las metas y plazos se cumplan conforme a lo planificado.

Además, la Oficina Asesora de Planeación y Finanzas será un punto de apoyo fundamental para fortalecer las actividades ejecutadas, brindando el soporte necesario en la asignación de recursos, la priorización de tareas y la alineación de los objetivos estratégicos del Ministerio con las iniciativas de seguridad digital y privacidad de la información. Este monitoreo constante también contribuirá a la mejora continua del plan, permitiendo ajustes según las necesidades y condiciones cambiantes del entorno organizacional.

PLAN DE MEJORAMIENTO CONTINUO

A continuación, se detallan las actividades que se desarrollarán para fortalecer el modelo de seguridad y privacidad de la información actual del Ministerio de Educación Nacional.

IDENTIFICACIÓN, ACTUALIZACIÓN Y ACEPTACIÓN DE ACTIVOS DE INFORMACIÓN

Al momento de generar controles de seguridad, es fundamental conocer previamente qué activos de información se deben proteger. Por ello, como paso inicial, es necesario realizar una capacitación con los enlaces, quienes son las personas designadas por los directivos de cada área y tienen un conocimiento profundo de los procesos del Ministerio. Esta capacitación permitirá identificar o actualizar los activos de información que aportan valor agregado a los procesos y, por lo tanto, requieren protección frente a potenciales riesgos.

Una vez identificados los activos de información, se procederá a su clasificación, utilizando la triada de confidencialidad, integridad y disponibilidad (CID). Esta clasificación garantiza que cada activo reciba el nivel de protección adecuado según su criticidad. Posteriormente, se elaborará la matriz de activos, la cual debe ser publicada en el Sistema Integrado de Gestión (SIG) para su gestión continua y control.

Para llevar a cabo esta capacitación, es necesario verificar si existe alguna nueva reglamentación aplicable al procedimiento vigente en la entidad. Esto garantizará que cualquier ajuste o actualización en el proceso se realice conforme a la normativa actual, y que la publicación en el SIG cumpla con los requisitos legales y organizacionales.

Las tareas clave que se desarrollarán en este proceso son las siguientes:

- Definir enlaces de cada proceso institucional para identificación de activos.

- Actualizar metodología en caso de ser necesario.
- Capacitar a los enlaces sobre la metodología a aplicar.
- Actualizar activos de información.
- Validar la actualización realizada.
- Consolidar la información recopilada y cargarla en el SIG.
- Aceptación de la clasificación de los activos de información por parte de los lideres de los procesos institucionales.
- Publicar los activos de información en los sistemas correspondientes.

APROPIACIÓN DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para que un modelo de seguridad y privacidad de la información tenga resultados exitosos, es necesario que todos los lineamientos se socialicen con los colaboradores de la entidad, para promover una cultura digital, atentos a los riesgos de seguridad digital en las labores diarias, dentro de las instalaciones del Ministerio o en la modalidad de teletrabajo.

Por lo anterior es necesario definir, por medio del formato de toma de conciencia (PM-FT-18) del Sistema Integrado de Gestión, las temáticas que serán socializadas por los diferentes medios dispuestos por el Ministerio, entre los cuales se encuentran el Pregonero y RadioMEN.

Es importante, así mismo, realizar ejercicios de ingeniería social para evaluar el nivel de conciencia de los usuarios finales con respecto a mensajes falsos con los cuales puede comprometer la seguridad de la información de los activos que maneja.

Las tareas que se desarrollarán son:

- Definir temáticas a sensibilizar.
- Diligenciar formato de toma de conciencia.
- Crear piezas de sensibilización para enviar por los medios dispuestos.
- Enviar piezas de sensibilización.
- Realizar ejercicios de ingeniería social.

PLAN DE RECUPERACIÓN DE DESASTRES

Con el objetivo de minimizar las afectaciones derivadas de la materialización de un riesgo de seguridad digital, es fundamental llevar a cabo una actualización de la estrategia de recuperación ante desastres. Para ello, se debe comenzar con la

actualización del Análisis de Impacto en el Negocio (BIA), el cual permitirá identificar los sistemas críticos y priorizar aquellos que requieren recuperación inmediata en caso de un incidente.

Una vez actualizado el BIA, se procederá a revisar y actualizar la estrategia del Plan de Recuperación ante Desastres (DRP) tecnológicos, asegurando que incluya procedimientos claros y efectivos para la recuperación de los sistemas más críticos. Además, se establecerá una metodología para probar periódicamente la efectividad del DRP, asegurando que los mecanismos de recuperación estén alineados con las necesidades de la organización y preparados para responder ante cualquier contingencia.

Una vez completada la actualización del BIA y el DRP, será necesario publicar la información actualizada en el Sistema Integrado de Gestión (SIG), garantizando su accesibilidad y disponibilidad para todos los interesados, así como su inclusión en los procesos de gestión continua de riesgos.

Las tareas que se desarrollarán son:

- Actualizar documentación del Análisis de Impacto del Negocio.
- Actualizar la documentación de estrategias del plan de recuperación de desastres tecnológicos.
- Realizar pruebas de las estrategias del plan de recuperación tecnológicos.
- Ajustar documentación de la estrategia de ser necesaria de acuerdo con la tarea anterior.

AUDITORÍAS

Una parte esencial para mejorar el Modelo de Seguridad y Privacidad de la Información (MSPI) es la realización de auditorías periódicas a las políticas y controles establecidos en la Declaración de Aplicabilidad. Estas auditorías permiten identificar oportunidades de mejora y asegurar que los controles implementados siguen siendo efectivos frente a los riesgos actuales.

Por este motivo, la Oficina de Tecnología y Sistemas de Información participará activamente en estas sesiones de auditoría y en los planes de mejora que se deriven de ellas. En caso de encontrarse oportunidades para optimizar los controles o procesos, se implementarán las acciones correctivas y preventivas necesarias para garantizar el cumplimiento de los objetivos de seguridad de la información.

Este enfoque asegura una mejora continua del MSPI, promoviendo un entorno de seguridad robusto que se ajusta a las necesidades y retos actuales del ministerio.

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Participar activamente en las sesiones de los comités directivos con el fin de presentar los avances realizados en el Modelo de Seguridad y Privacidad de la Información (MSPI), así como en los planes de mejoramiento y los indicadores de desempeño establecidos en el Sistema Integrado de Gestión (SIG). Durante estas sesiones, se expondrán los progresos alcanzados, las áreas de mejora identificadas y los planes de acción implementados, con el objetivo de recibir la retroalimentación correspondiente por parte del comité directivo.

La participación en estos comités asegura una alineación estratégica entre las iniciativas de seguridad de la información y los objetivos globales de la entidad, fomentando la toma de decisiones informada y el apoyo institucional a las acciones necesarias para fortalecer la seguridad digital.

ACTUALIZACIÓN Y CREACIÓN DE DOCUMENTACIÓN SGSI

Actualizar, cuando sea necesario, la documentación referente a los manuales, políticas y procedimientos, garantizando su publicación en el Sistema Integrado de Gestión (SIG) para asegurar su accesibilidad y cumplimiento.

Las tareas por desarrollar para cumplir con este objetivo son:

- Validar las políticas y procedimientos existentes.
- Actualizar políticas y procedimientos en caso de ser necesario.
- Publicar las políticas y/o procedimientos con los ajustes correspondientes.

REVISIÓN DE CONTROLES

Validar el cumplimiento de los controles físicos y lógicos establecidos en la política general de seguridad de la información definida en el Ministerio y que está reflejada en la declaración de aplicabilidad. Además, se deberán ejecutar acciones correctivas o de mejora en caso de que se identifiquen desviaciones o ineficiencias en los controles establecidos.

Las tareas por desarrollar para cumplir con este objetivo son:

- Validar la correcta implementación de los controles. definidos Realizar ajuste a los controles en caso de ser necesario.

Por lo tanto, es fundamental validar al inicio de cada vigencia las actualizaciones del instrumento de MinTIC, con el fin de adoptar las medidas necesarias y ajustar el plan de seguridad en función de las nuevas disposiciones, cambios normativos o actualizaciones tecnológicas que puedan surgir.

Este proceso garantizará que el plan se mantenga alineado con las directrices y requisitos regulatorios más recientes, fortaleciendo la gestión de riesgos y el cumplimiento normativo en el Ministerio.

PROGRAMA DE RESPONSABILIDAD DEMOSTRADA

Establecer, implementar y mantener un programa integral de gestión de protección de datos personales que garantice el cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 1081 de 2015, las directrices de la SIC y los estándares internacionales aplicables, fortaleciendo la cultura institucional de privacidad y asegurando el tratamiento legítimo, seguro y transparente de los datos personales administrados por el MEN**.**

CONTROL DE CAMBIOS

Control de Cambios		
Versión	**Fecha**	**Observaciones**
1	15 de Enero 2024	Se crea el documento de conformidad con los lineamientos institucionales establecidos y la normatividad vigente.
2	26 de Enero 2024	Aprobado en Comité Institucional de Gestión y Desempeño.
3	10 de Enero 2025	Se realiza modificación de la introducción, alcance, normativa y metodología, cumplimiento de la implementación y se ajustó el plan de mejoramiento continuo.
4	29 de Diciembre de 2025	Se realiza modificación de la introducción, alcance, normativa y metodología, cumplimiento de la implementación y se ajustó el plan de mejoramiento continuo.