Educación

PLANES ESTRATÉGICOS 2025

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Somos la Revolución del Cambio

Tabla de contenido

Introducción

El Ministerio de Educación Nacional en cumplimiento con lo indicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, en la resolución 500 de 2021y el decreto 338 de 2022 donde indica los lineamientos a seguir sobre la gobernanza que se debe tener a nivel de seguridad digital y de esta manera llevar a cabo un tratamiento de riesgos adecuado para todos los activos de información que se tienen dentro de las entidades; lo cual se puede llevar a cabo adoptando la "Guía para la administración del riesgo y el diseño de controles en entidades públicas3" y de esta manera crear la estrategia para el tratamiento de riesgos para esta entidad.

La metodología de la guía permite fortalecer el Sistema Integrado de Gestión (SIG), donde se registran los riesgos, ya que permite administrar y prevenir su ocurrencia y potenciar las oportunidades de mejora identificadas.

El presente plan describe las actividades necesarias para llevar a cabo la identificación de riesgos de seguridad digital sobre los activos de información, la creación de controles y planes de mejora con su debido seguimiento para aplicar el correspondiente tratamiento de riesgos enmarcado en las siguientes categorías:

Aceptar el riesgo: la entidad decide después de un análisis no adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo. Esta opción se puede considerar para riesgos con nivel bajo, sin embargo, se pueden presentar riesgos con otro nivel a los cuales la entidad no puede aplicar controles o planes para reducir el riesgo y es necesario aceptarlo. La aceptación del riesgo no implica que se olvide, sino que se debe hacer un seguimiento continuo del mismo.

Reducir el riesgo: se generan controles y/o planes de mejora orientados a disminuir tanto la probabilidad como el impacto de los riesgos identificados. Estas medidas se alinean con las buenas prácticas establecidas en la norma ISO/IEC 27002, que ofrece un marco sólido para gestionar la seguridad de la información. Dentro de estas acciones, se

promueve la segregación de funciones, el registro adecuado de actividades, auditorías internas y la implementación de controles específicos como la gestión de accesos, la protección de datos y la monitorización continua.

Evitar el riesgo: La entidad puede optar por eliminar el riesgo al interrumpir o modificar las actividades que lo generan. Esta estrategia implica cesar completamente la ejecución de procesos o actividades que puedan exponer a la organización a un riesgo no deseado, o bien cambiar la naturaleza de dichos procesos para que no representen una amenaza.

Compartir el riesgo: La entidad puede optar por compartir el riesgo a través de dos mecanismos principales. El primero consiste en externalizar o tercerizar la operación de ciertas actividades que generan riesgos, transfiriendo la gestión de esos riesgos a un proveedor especializado o un socio estratégico que cuente con las capacidades necesarias para mitigarlos de manera efectiva. El segundo mecanismo es la contratación de un seguro, que permite transferir financieramente las consecuencias de un posible incidente a una aseguradora. Ambos enfoques requieren una evaluación cuidadosa de los contratos, acuerdos de nivel de servicio (SLA) y pólizas, para asegurar que las responsabilidades estén claramente definidas y que el nivel de protección ofrecido sea adecuado para la naturaleza del riesgo compartido.

Objetivos

- Realizar un proceso de mejora continua para el tratamiento de riesgos de seguridad digital.
- Aplicar los lineamientos indicados en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" y procesos internos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información y de esta manera propender por la integridad, confidencialidad y disponibilidad.
- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.
- Fortalecer y apropiar al personal del Ministerio de Educación sobre el tratamiento de riesgos de seguridad digital.

Referencias Normativas

El Ministerio de Educación Nacional, "en cumplimiento de lo establecido en el artículo 2.2.21.1.6 del Decreto 648 de 2017 en lo que respecta a la aprobación de la política de administración del riesgo y el "artículo2.2.21.5.4 Administración de riesgos" del Decreto 1083 de 2015, y Siguiendo las directrices de las normas internacionales y marcos normativos aplicables, como la ISO 37001:2016 (Sistemas de Gestión Antisoborno), ISO 27001:2013 e ISO 27001:2022 (Sistemas de Gestión de Seguridad de la Información), así como la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas, versión 5, emitida por el Departamento Administrativo de la Función Pública, y el Decreto 1499 de 2017, que establece el Modelo Integrado de Planeación y Gestión (MIPG), se ha desarrollado la Guía de Administración del Riesgo PM-GU-01. La cual proporciona un conjunto de directrices detalladas que deben seguirse para la gestión y tratamiento de riesgos de manera transversal en la organización, abarcando diversas áreas clave y menciona todas las directrices que se deben seguir al momento de realizar el tratamiento de riesgos de manera transversal y se dedica una sección para el tratamiento de riesgos de seguridad digital, iniciando desde la identificación de activos de información y finalizando con el tratamiento de riesgos para estos activos, todo esto a su vez apoyados con el Procedimiento de Administración de Riesgos PM-PR-11, documentos que su última fecha de modificación corresponde a 14 de agosto de 2024 y 6 de agosto de 2024 respectivamente.

Textos y Definiciones

Activos de información: en el contexto de la seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenaza: causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Riesgo cibernético: posibilidad de que se materialice una falla en la seguridad de los componentes tecnológicos o servicios de información, sistemas de control, sistemas electrónicos y las telecomunicaciones que por ataques o intrusiones podrían impactar la movilidad de personas, alimentos, mercancías peligrosas y elementos esenciales y de carácter vital.

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de activos: consiste en obtener el máximo rendimiento de los bienes o recursos, es decir de todo aquello que tenga valor para una organización.

Infraestructuras criticas cibernéticas- ICC: instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar de los ciudadanos.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial el orden institucional y los intereses nacionales, incluye aspectos relacionados con el aspecto físico, digital y las personas.

Seguridad digital: preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

Clasificación de Activos de información: orden y agrupación de los activos de información en función de los requisitos legales, valor, criticidad y susceptibilidad a la divulgación o a la modificación no autorizada de los recursos tecnológicos con los que cuenta una organización para agilizar su gestión.

Vulnerabilidad: representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

CVE: Es un programa para identificar, definir y catalogar las vulnerabilidades de seguridad cibernética divulgadas públicamente.

Enlace: son las personas designadas por los directivos de área para realizar la identificación de activos de información y la identificación y tratamiento de riesgos de seguridad digital.

Establecimiento Contexto

Con base en la identificación de los servicios proporcionados por el Ministerio de Educación Nacional y soportados en los activos de información que deben identificarse previamente, en segunda instancia, se debe estimar la probabilidad y el impacto de las amenazas identificadas para el contexto externo e interno del Ministerio de Educación Nacional, y que desarrolló el Manual del Sistema Integrado de Gestión PM- MA-01 con fecha de actualización 6 de agosto de 2024, es por ello la importancia de que cada enlace con el que se identifican riesgos, conozca el objetivo del proceso.

Dentro del contexto del Ministerio, se listan a continuación algunas amenazas que pueden llegar a impactar los objetivos y que deberán ser tenidas en cuenta al momento del tratamiento del riesgo para cada proceso:

- Enfermedad no profesional.
- Incidente de seguridad y salud en el trabajo. Interrupción de TI y telecomunicaciones. Ataque cibernético y violación de datos. Fenómenos meteorológicos extremos.
- Falta de talento/habilidades clave. Cambios normativos.
- Interrupción del suministro de servicios públicos. Violencia política/disturbios civiles.
- Introducción de nuevas tecnologías (IoT, IA, Big data). Fallas en infraestructura crítica.
- Cambios en el gobierno. Desastres naturales.
- Obsolescencia Tecnológica.
- Phishing y Spear Phishing.
- Exfiltración de datos.
- Insider threats.

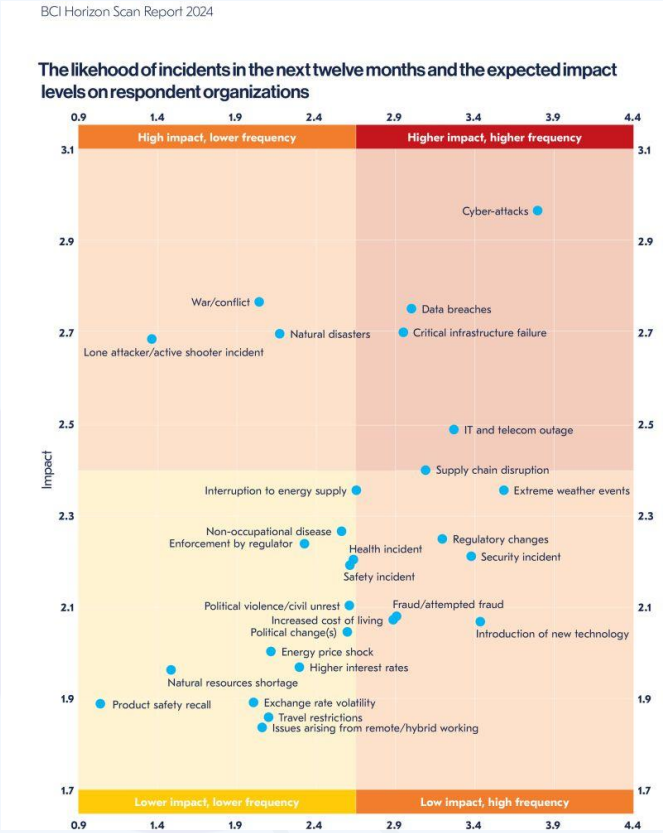
Información Sobre la Evaluación

El Ministerio de Educación Nacional mediante resolución 017564 del 31 diciembre 2019, adoptó el registro de activos de información, para cada uno de los procesos de la entidad y a su vez la gestión de los riesgos que puedan afectar el logro de los objetivos institucionales, la protección del medio ambiente, la seguridad de la información y el bienestar integral de los colaboradores. Para realizar el levantamiento de riesgos se cuenta con el procedimiento de administración de riesgos PM-PR-11, actualizado en 6 de marzo de 2024.

Los activos de información identificados deben estar tabulados con la siguiente información: dueño del activo, clasificación del activo, clasificación de la información y la criticidad de la información de acuerdo con los conceptos de confidencialidad, integridad y disponibilidad.

Un punto importante al momento de levantar riesgos es que, a nivel de seguridad de la información, existen solo tres tipos de riesgos: pérdida de confidencialidad, pérdida de integridad y pérdida de la disponibilidad. Sin embargo, existen varias vulnerabilidades y amenazas que pueden conllevar a la materialización de estos riesgos, haciendo necesario que se identifiquen las fuentes o factores de riesgo, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

Por ejemplo, en el reporte BCI Horizon Scan Report 2024, se listan los riesgos y las amenazas para América, lo cual es una fuente para que a nivel de los ejercicios de contexto del Ministerio se valide si alguna de estas amenazas puede tener una frecuencia alta e impactar los servicios prestados a la comunidad.



Fuente BCI Horizon Scan Report 2024

Valoración del riesgo, corresponde a la frecuencia de las actividades que se desarrollan y que son las que dan origen al riesgo:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V6", 2022

Posterior a ello se determina el criterio de impacto del riesgo y se especifica en términos del grado de daño o de los costos para el Ministerio, causados por un evento de seguridad de la información, registrándolo de la siguiente manera:

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V6", 2022.

Tratamiento del Riesgo

Conociendo los activos de información, su criticidad, y las implicaciones económicas, legales y reputacionales que puedan surgir por verse afectada la disponibilidad, integridad y confidencialidad de la información, se deben tomar algunas de las siguientes acciones para el tratamiento del riesgo:

Aceptar el riesgo: La entidad decide después de un análisis no adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo. Esta opción se puede considerar para riesgos con nivel bajo, sin embargo, se pueden presentar riesgos con otro nivel a los cuales la entidad no puede aplicar controles o planes para reducir el riesgo y es necesario aceptarlo. La aceptación del riesgo no implica que se olvide, sino que se debe hacer un seguimiento continuo del mismo.

Reducir el riesgo: Se generan controles y/o planes de mejora orientados a disminuir tanto la probabilidad como el impacto de los riesgos identificados. Estas medidas se alinean con las buenas prácticas establecidas en la norma ISO/IEC 27002, que ofrece un marco sólido para gestionar la seguridad de la información. Dentro de estas acciones, se promueve la segregación de funciones, el registro adecuado de actividades, auditorías internas y la implementación de controles específicos como la gestión de accesos, la protección de datos y la monitorización continua.

Evitar el riesgo: La entidad puede optar por eliminar el riesgo al interrumpir o modificar las actividades que lo generan. Esta estrategia implica cesar completamente la ejecución de procesos o actividades que puedan exponer a la organización a un riesgo no deseado, o bien cambiar la naturaleza de dichos procesos para que no representen una amenaza.

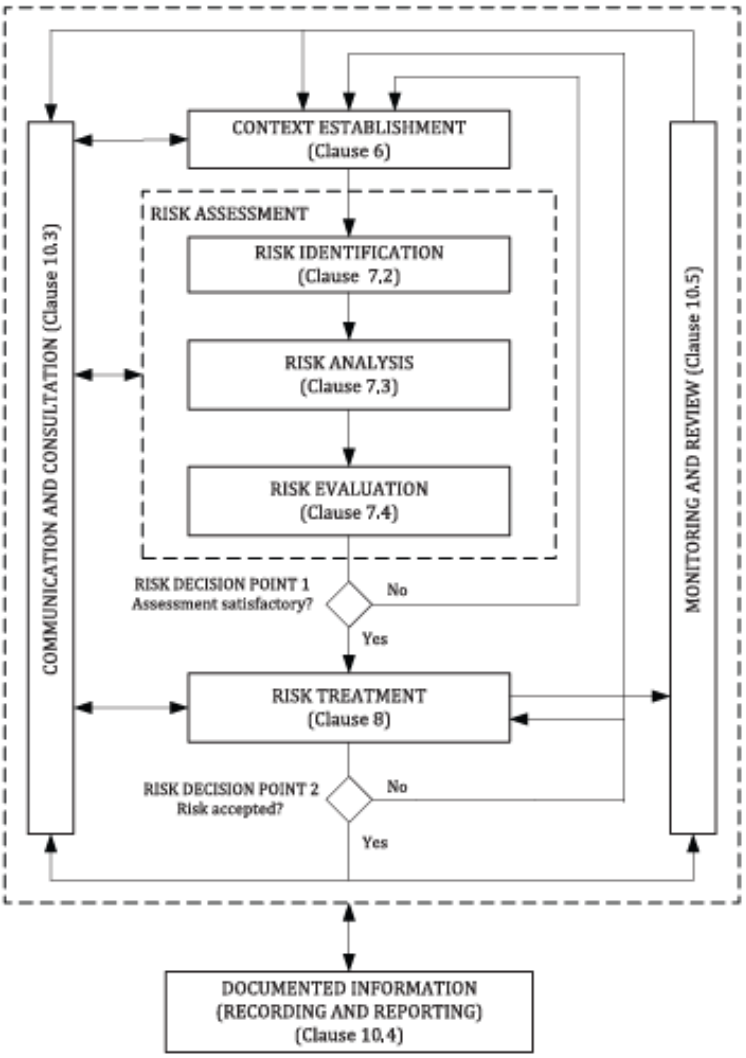
Compartir el riesgo: La entidad puede optar por compartir el riesgo a través de dos mecanismos principales. El primero consiste en externalizar o tercerizar la operación de ciertas actividades que

generan riesgos, transfiriendo la gestión de esos riesgos a un proveedor especializado o un socio estratégico que cuente con las capacidades necesarias para mitigarlos de manera efectiva. El segundo mecanismo es la contratación de un seguro, que permite transferir financieramente las consecuencias de un posible incidente a una aseguradora. Ambos enfoques requieren una evaluación cuidadosa de los contratos, acuerdos de nivel de servicio (SLA) y pólizas, para asegurar que las responsabilidades estén claramente definidas y que el nivel de protección ofrecido sea adecuado para la naturaleza del riesgo compartido.

Comunicación del Riesgo

La comunicación sobre el riesgo es una parte constante sobre todo el tratamiento de riesgos como lo expresa la norma NTC-ISO/IEC 27005:2022

ISO/IEC 27005:2022(E)



Fuente "ISO/IEC 27005

"Durante todo el proceso de gestión del riesgo en la seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los directores y al personal operativo correspondiente. Incluso antes del tratamiento de los riesgos, la información acerca de los riesgos identificados puede ser muy valiosa para la gestión de incidentes y puede ayudar a reducir el daño potencial. La toma de conciencia de los directores y el personal sobre los riesgos, la naturaleza de los controles establecidos para mitigar los riesgos y las áreas de interés para la organización facilitan el tratamiento eficaz de los incidentes y eventos inesperados. Se recomienda documentar los resultados detallados en cada actividad del proceso de gestión del riesgo en la seguridad de la información y de los dos puntos de decisión sobre el riesgo"5.

5 NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27005

Información de Seguridad

El seguimiento al tratamiento de riesgos no se limita únicamente a garantizar el cumplimiento de los controles existentes y la ejecución de los planes de mejora. Es esencial adoptar un enfoque de mejora continua, volviendo al inicio del proceso de gestión de riesgos para verificar si han surgido nuevos activos de información o si ha cambiado el contexto de los activos actuales. Esto implica ejecutar nuevamente el ciclo completo de tratamiento de riesgos, desde la identificación de activos y amenazas hasta la implementación de controles y mitigación de riesgos.

Del mismo modo, es crucial realizar una validación periódica de las amenazas, tanto internas como externas, que puedan afectar los objetivos del Ministerio de Educación Nacional. Un claro ejemplo de amenazas no anticipadas fue la pandemia, que afectó gravemente a múltiples sectores y evidenció la importancia de identificar proactivamente riesgos emergentes. La evaluación constante de estos factores ayuda a prevenir incidentes que podrían no haber sido considerados inicialmente.

Es igualmente relevante el análisis de escenarios en los que se materializan riesgos sin haber identificado previamente sus causas. En estos casos, el proceso de mejora continua en el tratamiento de riesgos adquiere mayor relevancia, ya que permite ajustar los controles y estrategias para evitar futuras ocurrencias similares. El seguimiento riguroso y la adaptación a cambios en el entorno de riesgo son fundamentales para mantener la resiliencia organizacional.

Además, deben revisarse de forma constante los criterios utilizados para medir los riesgos. Nuevas regulaciones, cambios en la criticidad de los activos o actualizaciones normativas pueden afectar la clasificación de un activo y, por tanto, su tratamiento. Algunos de los factores clave a tener en cuenta incluyen:

- Contexto legal y ambiental.
- Contexto de competencia en el mercado.

- Categorías y valor de los activos.
- Criterios de impacto.
- Criterios de evaluación del riesgo.
- Criterios de aceptación del riesgo.
- Costo total de la propiedad.
- Recursos necesarios.
- Enfoque para la valoración del riesgo.

Plan de Mejoramiento

A continuación, se detallan las actividades que se desarrollarán para fortalecer el tratamiento de riesgos de seguridad digital para los activos de información del Ministerio de Educación Nacional.

PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

La oficina de control interno y la subdirección de desarrollo organizacional coordinarán si es necesario la actualización de la política de administración de riesgos y las fechas de corte para el registro y monitoreo.

ESCANEO DE VULNERABILIDADES

Programar y realizar el escaneo de vulnerabilidades sobre el total de los servicios de información, el cual se realizará con una herramienta comercial y con la última versión disponible. La calificación de las vulnerabilidades se realiza a través del Common Vulnerabilities and Exposure - CVE; en los casos cuando la vulnerabilidad no se encuentra en CVE, pero ha sido confirmada por el fabricante, la clasificación se realizará directamente por la herramienta de escaneo de vulnerabilidades. El insumo para la mitigación de vulnerabilidades es el reporte de la herramienta, la cual indica la descripción y posible solución.

MITIGACIÓN DE VULNERABILIDADES

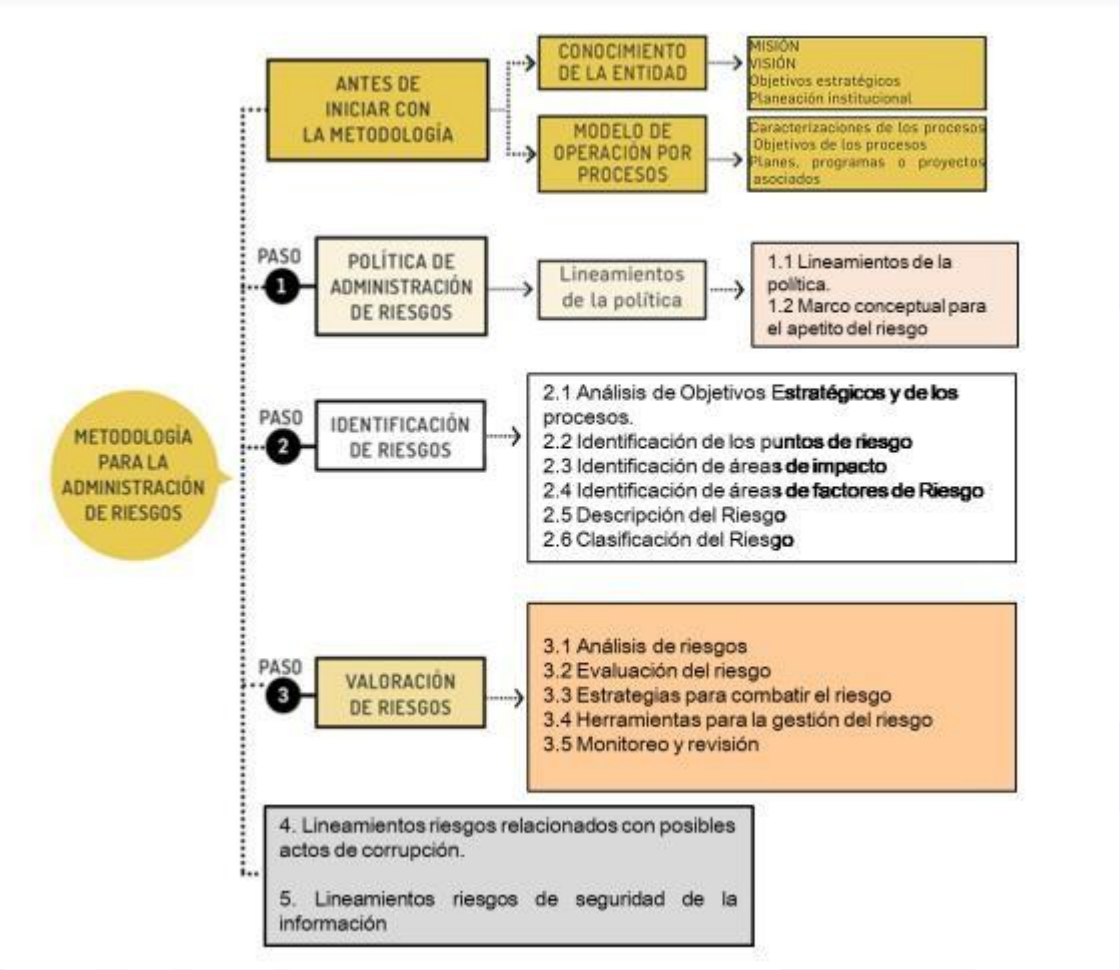
Basado en el reporte del escaneo de vulnerabilidades se prioriza la remediación iniciando con las vulnerabilidades de riesgo crítico y alto. En caso de no poder realizar una mitigación, se validarán controles o medidas necesarias para evitar la explotación de estas.

SOCIALIZACIÓN DEL ESTADO ACTUAL DE LOS SERVICIOS DE INFORMACIÓN

Socializar con los lideres funcionales y enlaces de activos de información el estado tecnológico de cada uno de los servicios de información de los cuales sean propietarios, con el fin de llevar a cabo planes de mejora o adquisición tecnológica según corresponda.

CAPACITACIÓN SOBRE RIESGOS DE SEGURIDAD

Realizar capacitación a los enlaces definidos por los directivos de área para que puedan realizar la identificación de riesgos de seguridad digital, orientada bajo la siguiente metodología:



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS

Identificar los riesgos de seguridad digital basados en la capacitación realizada. Durante este proceso la Oficina de Tecnología y Sistemas de Información realizará los acompañamientos que se requieran a los enlaces, teniendo en cuenta que cada área tiene el conocimiento claro y preciso de su proceso y pueden identificar la forma en que la confidencialidad, integridad y disponibilidad, se pueden ver afectadas.

CREACIÓN DE PLANES DE TRATAMIENTO

Cuando el riesgo residual se mantenga en valores no aceptables según los criterios establecidos por la entidad, será necesario crear planes de tratamiento para reducir dicho riesgo, conforme a lo estipulado en la Guía de Tratamiento del Riesgo. Estos planes de tratamiento deben ser diseñados con el objetivo de implementar controles adicionales o mejorar los existentes, de manera que se logre mitigar la probabilidad o el impacto de los riesgos identificados hasta niveles aceptables para el ministerio.

CARGUE DE RIESGOS EN EL SIG

Cargar en el Sistema Integrado de Gestión los riesgos identificados para los activos de información con los respectivos controles actuales y los planes de mejora a realizar.

AJUSTAR MAPA DE RIESGOS

Validar los riesgos que se cargaron y de esta manera ajustar el mapa de riesgos con la información entregada por cada dependencia.

SEGUIMIENTO A LOS CONTROLES Y PLANES DE MEJORAMIENTO

Realizar seguimiento a la información cargada por parte de cada área con respecto a los controles y planes de mejora para cada trimestre del año. Este seguimiento es clave para evaluar el progreso y la efectividad de las acciones adoptadas en la mitigación de riesgos y el fortalecimiento de la seguridad de los activos de información.

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 de Gestión y Desempeño
3	10 de Enero 2025	Se realiza actualización del seguimiento al tratamiento de riesgos, identificación de riesgos de seguridad digital, planes de tratamiento y validación en el Sistema Integrado de Gestión.