PLAN INSTITUCIONAL
DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIGSA 2021

SGSI
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Octubre 2020	Versión Inicial. Elaboración por primera vez del documento.
2	Enero 2021	Describa aquí los cambios que le hizo al documento en relación a la versión anterior. NOTA PROASIG - PROPLAES: Este Plan fué aprobado en sesión de Comité de Gestión y Desempeño Institucional, del que hacen parte el Director General de Sanidad Militar, los Subdirectores de Salud, Técnico y de Gestión, y Administrativo y Financiero de la DIGSA, los Directores de Sanidad del Ejército y Armada Nacional, Jefatura de Salud de la Fuerza Aérea y los Coordinadores de Grupo de Planeación Estratégica, Asuntos Legales y Seguimiento y Evaluación de la DIGSA; y documentado mediante Acta N° 0120010254602, de fecha 16 de diciembre de 2020. El documento original está debidamente firmado, reposa en los documentos del proceso asociado y está disponible en, https://www.sanidadfuerzasmilitares.mil.co/, lo anterior en cumplimiento al Decreto 612 de fecha 4 de abril 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”.

CONTROL DE APROBACIÓN

Aprobó:	CR. Luis Hernando Sandoval Pinzón Subdirector Técnico y de Gestión de DIGSA	
Revisó:	CS. Vivian Tatiana Alba Díaz	CR. Carlos Darío Gonzalez Villamil

	Gestor de Calidad PROGTIC	Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección
Elaboró:	PD. Diana Marcela López Bejarano Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA	

Contenido

1. Presentación

La política de seguridad de la información de la Dirección General de Sanidad Militar, tiene como objetivo la protección de los activos de información ante una serie de amenazas o brechas que atenten contra los principios fundamentales de la seguridad, como lo son la perdida de la confidencialidad, integridad y Disponibilidad que posiblemente puedan afectar la continuidad de la DIGSA. Por ello mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se busca identificar las amenazas, las vulnerabilidades, el impacto y el nivel de riesgos asociados a los activos de información, así como el tratamiento, evaluación y monitoreo de los mismos.

Teniendo como referencia el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y el Sistema de Gestión de Seguridad de la Información – SGSI que se encuentra en proceso de implementación en la Dirección General de Sanidad Militar y basados en un enfoque de planeación de gestión del riesgo, se busca prevenir los efectos no deseados que puedan presentarse en cuanto a seguridad de la información; por lo cual es importante establecer y controlar la gestión de incidentes que afecten los activos de información e implantar unas contramedidas para disminuir la probabilidad de su materialización.

Lo anterior se realiza en cumplimiento a la normatividad establecida por el estado colombiano, a través del CONPES 3854 DE 2016, el Modelo de Seguridad y Privacidad de MINTIC, el decreto 1008 de 14 de junio 2018 y adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.

2. Objetivos del Plan Tratamiento de Riesgos Seguridad y Privacidad de la Información

2.1 Objetivo General

Establecer las actividades que se planean realizar para analizar, evaluar y tratar los riesgos de Seguridad de la Información a los que pueda estar expuesta la Dirección General de Sanidad Militar, alineados con las políticas de seguridad y privacidad de la información, para de esta manera proteger y preservar la integridad, confidencialidad, disponibilidad y autenticidad de la información.

2.2 Objetivos Específicos

- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información al interior de la DIGSA.

- Identificar las principales amenazas que afectan a los activos de información de la DIGSA
- Involucrar y comprometer a todos los funcionarios de la DIGSA en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos de seguridad de la información.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

3. Alcance

La identificación y tratamiento de los riesgos de seguridad de la información como plan institucional, busca realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información que permita integrar en los procesos de la DIGSA, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos; dicho tratamiento de riesgos involucra a los procesos misionales y el proceso de apoyo relacionado con la Gestión Tecnológica y será de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la DIGSA.

4. Fundamento Normativo

- Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- Ley 1341 de 2009. “Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

- Decreto 1377 de 2013. “Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

- 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”. Decisión Andina 351 de 2015 “Régimen común sobre derecho de autor y derechos conexos”.

- Decreto 2573 de 2014 “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea…”, donde se encuentra como componente el Modelo de Seguridad y Privacidad de la Información.

- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

- Decreto 1413 de 2017 “Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.

- Norma Técnica Colombiana ISO27001:2013. Sistemas de Gestión de Seguridad de la Información.

- Norma Técnica Colombiana ISO31000:2013. Gestión del Riesgo Principios y Directrices.

- Directiva Permanente Nro. DIR2014-18 “Políticas de Seguridad de la Información para el Sector Defensa”.

- Directiva Permanente No. 154 /MDN-CGFM-JEMC-SEMCO-JEIMC-DIRCO-23.1 “Políticas de Seguridad de las Información para las Fuerzas Militares”.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital año 2018.

5. Definiciones

Amenaza: Causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Calificación del riesgo: Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Causa: Medios, circunstancias y/o agentes que generan riesgos.

Compartir o transferir el riesgo: Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como seguros o sitios alternos.

Consecuencia: Efectos que se pueden presentar cuando un riesgo se materializa.

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

Evaluación del riesgo: Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Evitar el riesgo: Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados.

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Mapa de riesgos: Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Materialización del riesgo: Ocurrencia del riesgo identificado.

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.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Propietario de activo de información: Identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Responsable del tratamiento: 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.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos de la DIGSA. Se expresa en términos de probabilidad y consecuencias.

Riesgo residual: Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

Valoración del riesgo: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

6. Recursos

La Dirección General de Sanidad Militar en el marco de la Gestión de Riesgos de Seguridad y Privacidad de la Información, dispone de los siguientes recursos:

No.	Recursos	Variable
1.	Humanos	El Grupo Sistema Integral de Información–Tecnologías de la Información y las Comunicaciones a través del Área de Seguridad de la Información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la DIGSA en lo concerniente a la seguridad y privacidad de la información.

No.	Recursos	Variable
2.	Técnicos	Guía para la Administración del riesgo y el diseño de controles en entidades públicas, versión 4 del Departamento Administrativo de la Función Pública. Guía de Gestión de Riesgos del Ministerio de las Tecnologías de la Información y Comunicaciones

Ilustración 1. Proceso Administración del riesgo

7. Presupuesto

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la DIGSA, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

8. Metodología para el Tratamiento de Riesgos Seguridad y Privacidad de la Información

La metodología para el tratamiento de riesgos de seguridad y privacidad de la información de la DIGSA, se basa en la guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública a través del anexo 4. “Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas”, así como los lineamientos para la gestión de riesgos de seguridad digital en entidades públicas establecidos por el MinTIC.

La siguiente ilustración muestra el proceso de gestión del riesgo de seguridad de la información.

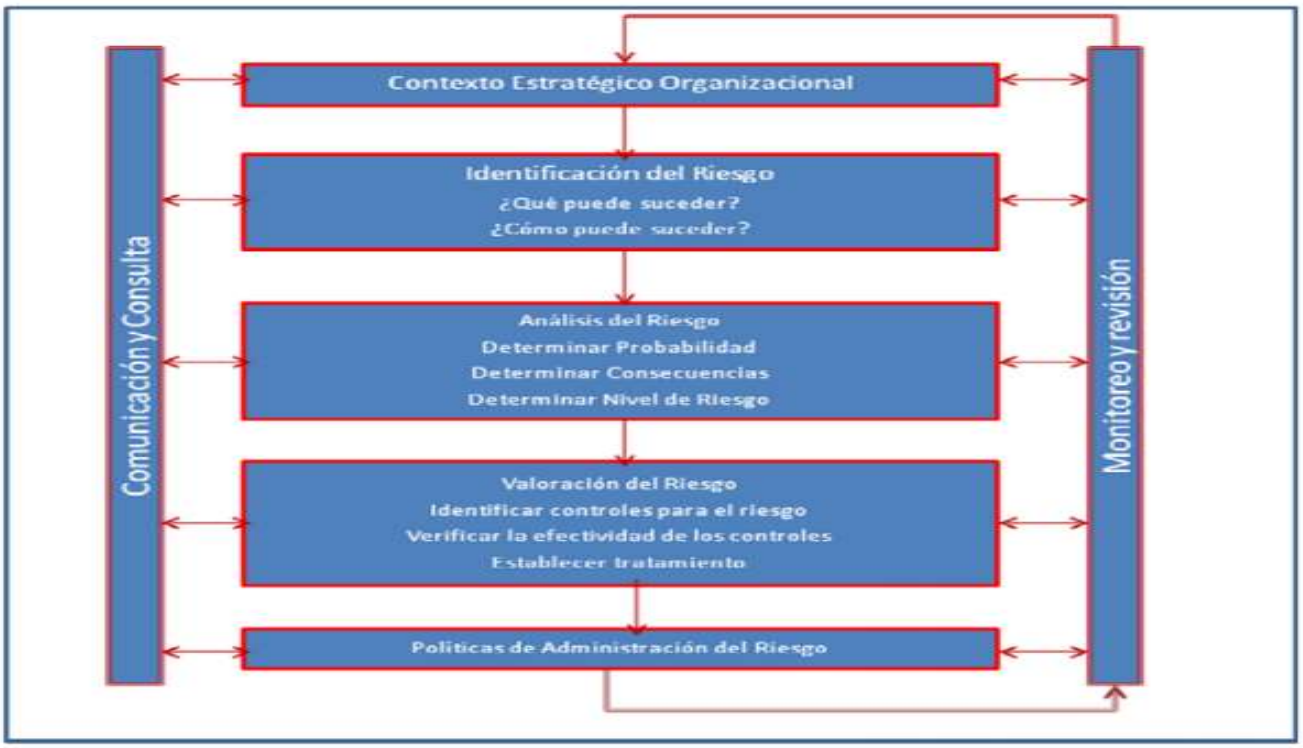

Ilustración 1. Proceso Administración del riesgo
Fuente: Cartilla Administración del Riesgo DAFP

Conforme a lo anterior la Dirección General de Sanidad Militar, se encuentra en la fase de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), en donde se integran tareas asociadas a la gestión de riesgos de seguridad digital, como se demuestra en la siguiente ilustración donde se observa la Interacción entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo de Gestión de Riesgos de Seguridad Digital (GRSD).

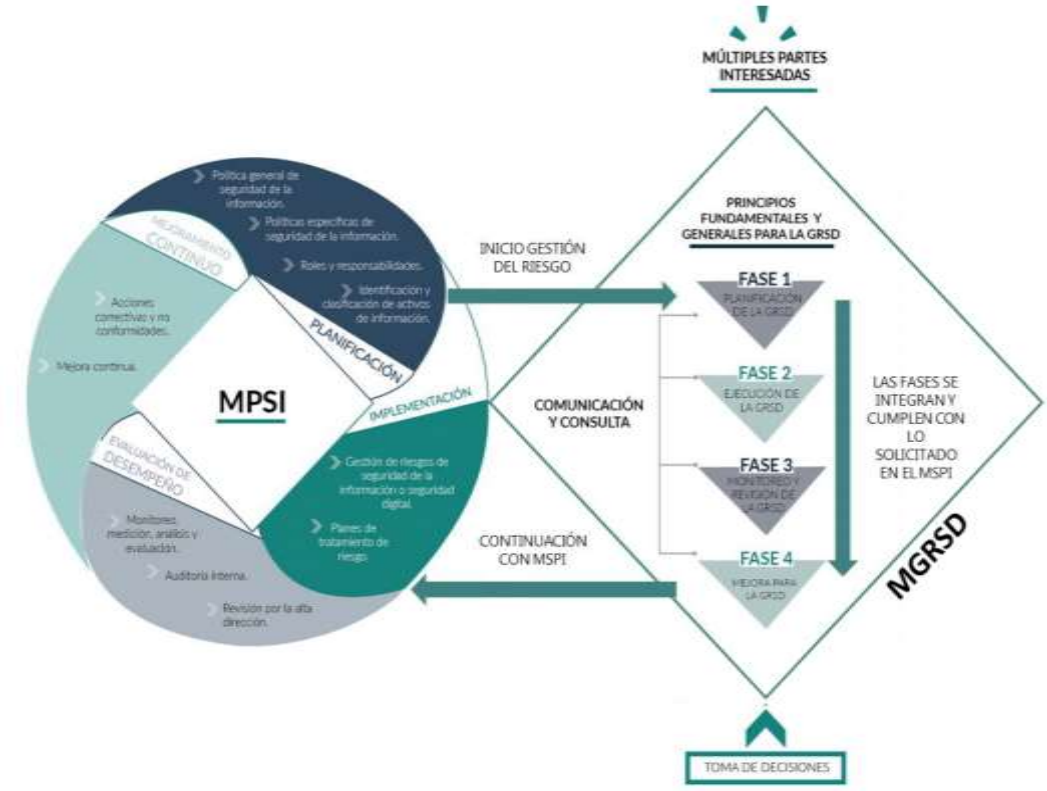

Ilustración 2. Interacción entre el MSPI Y EL MGRSD
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

9. Etapas para la Gestión del Riesgo

   a. Contexto Estratégico

      Define los criterios básicos basándose en la Identificación de los activos de información, valoración de riesgos asociados a los activos de información de los procesos establecidos en el alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Así mismo el establecimiento y calificación de los controles para la obtención de los riesgos residuales de los procesos evaluados.

   b. Criterios de Evaluación de Riesgos de Seguridad de la Información

      La evaluación de los riesgos de seguridad de la información se enfocará en:

      - El valor estratégico del proceso de información en la DIGSA
      - La criticidad de los activos de información involucrados.

- Los requisitos legales y reglamentarios.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la DIGSA.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Agencia.

c. Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la DIGSA, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

d. Valoración de los Riesgos de Seguridad de la Información

Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información. Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la DIGSA, en esta fase se realizan las siguientes actividades:

- Análisis del riesgo: Se realiza la identificación de los riesgos y la estimación del riesgo.

- Evaluación del riesgo: La evaluación del riesgo requiere de una evaluación de los controles existentes.

e. Tratamiento de Riesgos de Seguridad de la Información

Se elaborará el mapa de riesgos de seguridad de la información, una vez los procesos descritos en el alcance de la DIGSA, hayan realizado la Identificación y valoración de activos de seguridad de la información y basado en ello hayan realizado la administración de riesgos.

Seguidamente se hace una consolidación de todos los tratamientos que hayan sido determinados por los procesos con las decisiones establecidas: si se optó por tomar el riesgo, si se va a reducir, se va a transferir o evitar el riesgo. En caso que la decisión sea

reducirlo, se documenta aquí las medidas de seguridad digital que se van a seleccionar y aplicar, la innovación o las medidas de preparación para su tratamiento.

Es de anotar que se debe tener la aprobación del plan de tratamiento de riesgos por parte de los dueños de cada riesgo, que en este caso corresponderían a los dueños de los procesos.

f. Monitoreo y seguimiento de los riesgos de seguridad de la información

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información. Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos.
- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos,
- Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

10. Actividades Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Teniendo en cuenta que mediante resolución No. 0322 del 11 de marzo del 2020, se crean y organizan grupos Internos de trabajo en la Dirección General de Sanidad Militar, para la vigencia del 2021 se debe realizar cada una de las etapas del proceso de gestión de riesgos en las áreas misionales y de tecnología de la DIGSA, con el fin de actualizar las matrices de riesgos de seguridad de la información, la calificación de probabilidad e impacto, los controles existentes y los planes de tratamiento de riesgos por parte de cada uno de los líderes de proceso. A continuación, se describen las actividades que se van a realizar en la vigencia 2021, así:

No.	Actividad	Responsables	Evidencia actividad	Fecha
1	Actualizar el inventario de activos de información de los procesos definidos en el alcance del SGSI.	Área Seguridad de la Información. Líder o responsable asignado por el proceso	Matriz de Inventario de Activos de Información.	Enero-Marzo

No.	Actividad	Responsables	Evidencia actividad	Fecha
2	Asistir a mesas de trabajo para identificar los riesgos transversales de seguridad digital de la DIGSA.	Grupo Planeación Estratégica-Área Desarrollo Institucional Área Seguridad de la Información. Líder o responsable asignado por el proceso	Actas de reunión	Enero-Marzo
3.	Monitorear la efectividad de los controles existentes.	Grupo Planeación Estratégica-Área Desarrollo Institucional Área Seguridad de la Información.	Informe de Monitoreo de riesgos de seguridad de la información	Trimestral

Ilustración 3. Actividad Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

11. Aprobación y publicación

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información– PTRSPI deberá ser presentado y aprobado por el Comité Institucional de Gestión y Desempeño creado mediante Resolución No. 0129 de 2019[1].

[1] Resolución No. 0129 de 2019 “por el cual se crea el Comité de Gestión y Desempeño en la Dirección General de Sanidad Militar DIGSA, se conforma el Equipo MIPG – MECI, y se establecen otros lineamientos”.

12. Bibliografía

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PBLICA (2018). Guía para la Administración del riesgo y el diseño de controles en entidades públicas, versión 4. Bogotá.

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES, Guía de Gestión de Riesgos, https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION – ICONTEC. Norma Técnica Colombiana NTC/ISO/31000(2018). Gestión del Riesgo. Bogotá D.C.

12. Anexos