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

DIGSA 2022

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	Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, documentado mediante Acta N° 0120010254602, de fecha 16 de diciembre de 2020.
3	Enero 2022	Se actualizaron las actividades a desarrollar durante el año 2022. Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, documentado mediante Acta N° 0121013721902, de fecha 27 de diciembre de 2021. NOTA PROASIG – PROPLAES - PROALEG: Este documento fue revisado por PROASIG, cumple con los requisitos establecidos en el formato establecido por el Sistema Integrado de Gestión SIG, para aprobarlo en la SVE; PROPLAES libera el documento. Dada la reestructuración de la DIGSA, se ajustaron las políticas de operación para el control de la información documentada de los procesos para el SIG. La información registrada en el documento es responsabilidad del proceso que lo emite.

CONTROL DE APROBACIÓN

Aprobó:	CR. Santiago Murillo Colmenares Subdirector Técnico y de Gestión de DIGSA	
Revisó:	PD. Harlen Milena Moreno Alfonso Gestor de Calidad PROGTIC	CR. José Mauricio Barrera Barrera Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA (E)
	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

Ilustraciones

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.

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

3. Alcance

Orientar a los funcionarios de la Dirección General de Sanidad Militar en la identificación y el tratamiento de los riesgos de seguridad de la información, teniendo como fundamentos la metodología definida por el Departamento Administrativo de la Función Pública -DAFP y la Norma Técnica Internacional ISO 31000:2018; para de esta manera proteger y preservar la integridad, confidencialidad, disponibilidad y autenticidad de la información.

4. Fundamento Normativo

Fecha	Descripción
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
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 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
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	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Fecha	Descripción
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Directiva Permanente No. 154 /MDN-CGFM-JEMC-SEMCO-JEIMC-DIRCO-23.1	Políticas de Seguridad de las Información para las Fuerzas Militares.
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
Dirección de Gestión y Desempeño Institucional, diciembre 2020 – DAFP	Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5.
DIGSA Octubre del 2021	Guía para la Administración del Riesgo SSFM DIGSA

5. Definiciones

Concepto	Descripción
Acción	Proceso de realización de algo que implica cambio o movimiento. Se determina mediante verbos que indican la acción que deben realizar como parte del control.
Activo	En el contexto de 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, 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.
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.

Concepto	Descripción
Consecuencia	Efectos que se pueden presentar cuando un riesgo se materializa.
Control	Medida que permite reducir o mitigar el riesgo determinado por el proceso (políticas, dispositivos, prácticas u otras acciones).
Evaluación del riesgo	Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo
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.
Mapa de Riesgos	Documento que consolida la información resultante en cada una de las etapas de la Gestión 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
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	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales
Riesgo inherente:	Nivel del riesgo propio de la actividad, es aquel al que se enfrenta la entidad en ausencia de acciones para modificar su probabilidad o impacto

Concepto	Descripción
Riesgo residual	Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
Tolerancia al riesgo:	Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.
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.
2.	Técnicos	Guía para la Administración del riesgo y el diseño de controles en entidades públicas, versión 5 del Departamento Administrativo de la Función Pública. Guía para la Administración del Riesgo SSFM DIGSA.

Ilustración 1. Recursos 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 versión 5 de diciembre del 2020 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 Ministerio de Tecnologías de la Información y las Telecomunicaciones -MINTIC.

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

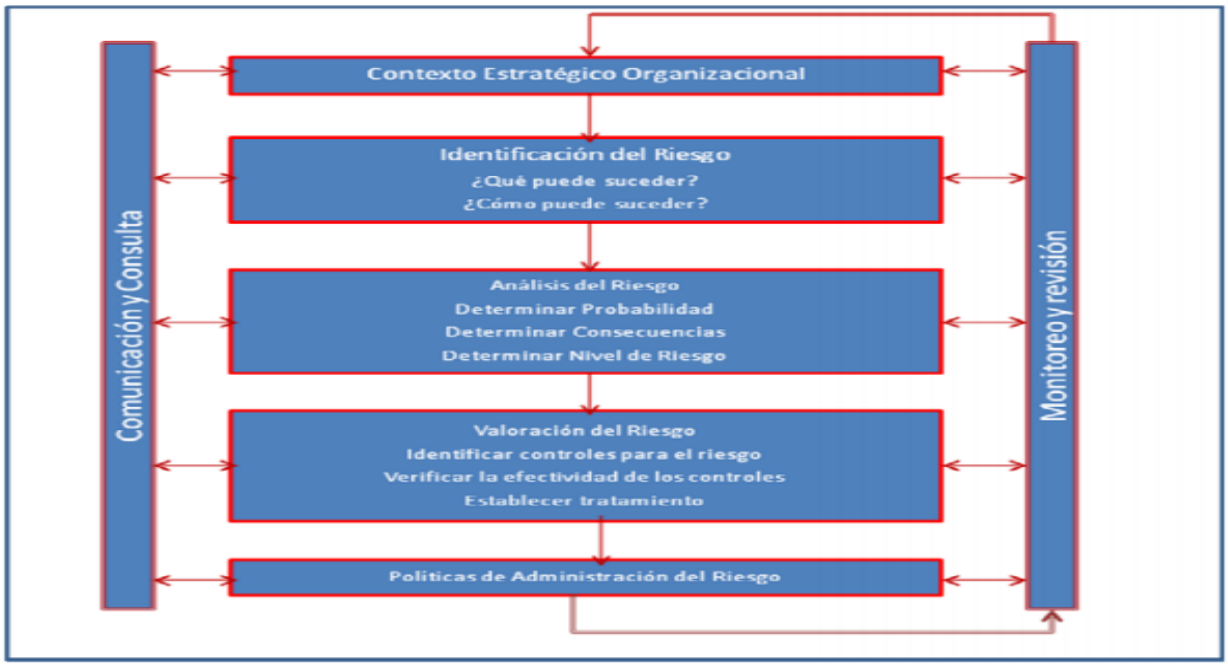


Ilustración 2. Proceso Administración Riesgo
Fuente: Cartilla Administración del Riesgo DAFP

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).

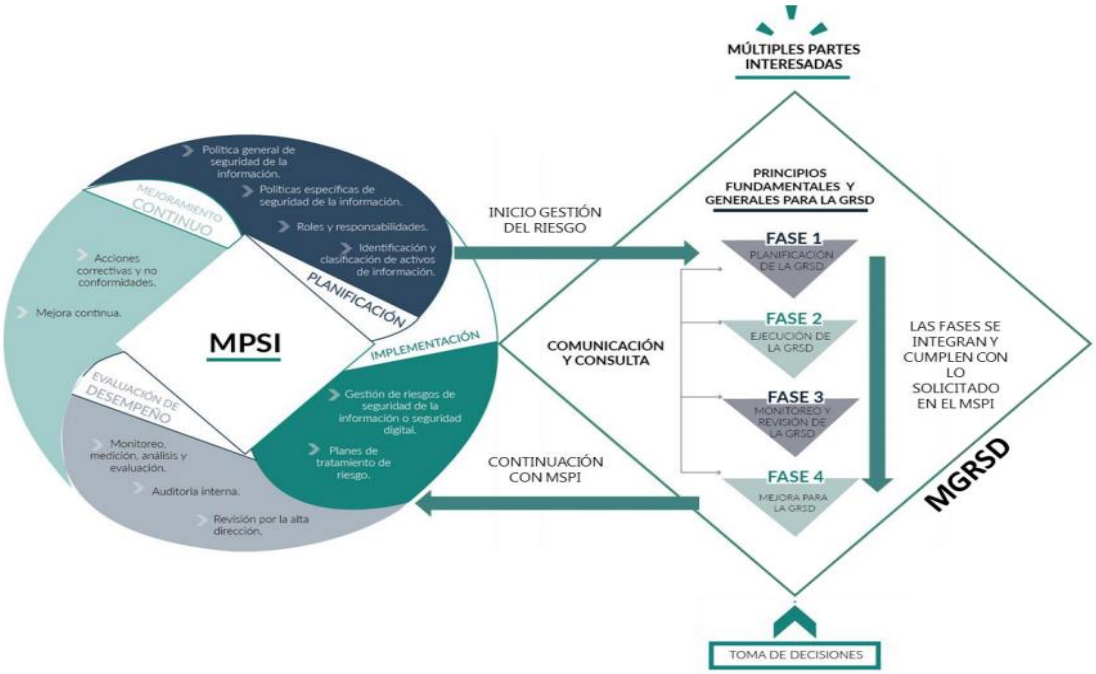


Ilustración 3. Interacción entre el MSPI y el MGRSD
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

9. Etapas para la Gestión del Riesgo

9.1 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.

9.2 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 DIGSA.

9.3 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

9.4 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:

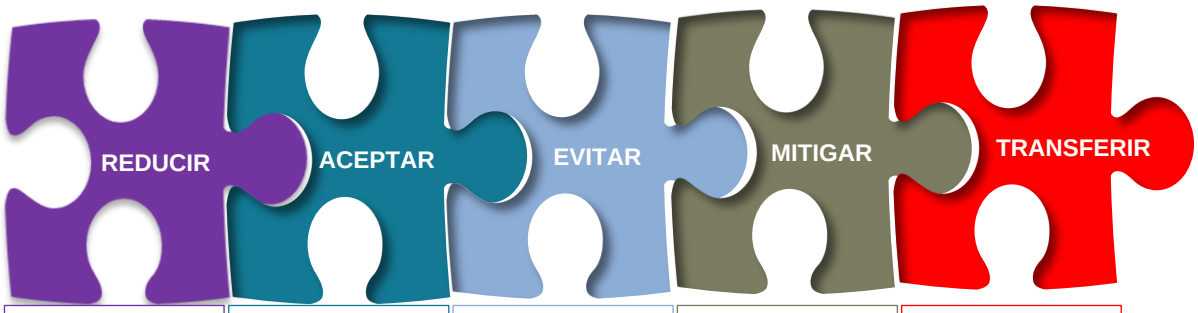
- Análisis del riesgo: Se realiza la identificación de los riesgos y la estimación del riesgo.

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

9.5 Tratamiento de Riesgos de Seguridad de la Información

Se define teniendo como base la Matriz de Activos de Información DIGSA código MDN-COGFM-PROGTIC-DIGSA-MT.95.1-1, una vez los procesos hayan realizado la Identificación y valoración de activos de seguridad de la información, se consolidará los riesgos de seguridad digital en el formato de Mapa de Riesgos Institucional DIGSA código MDN-COGFM-PROPLAES-DIGSA-FU.95.1-43.

Está claro que no todos los riesgos tienen el mismo nivel de criticidad y que su gestión implica una serie de esfuerzos y costos en los que debe incurrir la entidad, de ahí la importancia que los líderes de proceso evalúen las opciones existentes en materia de tratamiento del riesgo para la mitigación del riesgo, así como la relación costo-beneficio de las medidas de tratamiento, dicha decisión puede ser:



Adopta medidas para reducir la probabilidad o impacto, esto se determina mediante transferencia o mitigación.	No se adopta ninguna medida, se asume el mismo conociendo los efectos al materializarse.	Busca minimizar la probabilidad de materialización del riesgo.	Implementar acciones que mitiguen el nivel del riesgo, pueden estar asociadas al plan de acción*.	Reduce la probabilidad o el impacto, la mejor estrategia es tercerizar el proceso o trasladarlo a través de pólizas o seguros.

Ilustración 4.Estrategias para el manejo del riesgo
Fuente: Fuente: Elaborado y adoptado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas por el Grupo de Planeación – Desarrollo Institucional de la DIGSA.

9.6 Monitoreo y seguimiento de los Riesgos de Seguridad de la Información

En alineación con la dimensión 7 *"Control interno"* del Modelo Integrado de Planeación y Gestión – MIPG, se establece la responsabilidad y control, para la gestión del riesgo la cual es desarrollada por los funcionarios de la entidad.

- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos,
- Incidentes de seguridad de la información.

9.7 Modelo de las Líneas de Defensa

Establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos[1] como se describe en la tabla 7.

[1] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 75p

Línea de Defensa	Rol	Responsabilidad
Estratégica	•Alta Dirección •Subcomité Institucional de Coordinación de Control Interno.	Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad.
1ª	•Líderes de proceso y sus equipos.	• La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. • La gestión operacional identifica, evalúa, controla y mitiga los riesgos
2ª	•Planeación estratégica •Líder de proceso •Gestor de proceso	• Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. • Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
3ª	•Oficina de Control Interno o quien haga sus veces. •Auditoría Interna	La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporcionará aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.

Ilustración 5. Líneas de Defensa, Rol y Responsabilidad
Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 5. 60p.

9.8 Monitoreo

La entidad debe asegurar el logro de los objetivos, interesándose por el monitoreo y seguimiento periódico de los riesgos de la entidad (impactos, amenazas, vulnerabilidades y probabilidades), en busca de posibles cambios que requieran la valoración; esta acción debe ser realizada por el responsable o gestor del riesgo, anexando sus debidas evidencias de acuerdo con lo establecido en los controles.

Los riesgos son dinámicos, por tanto, podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión o monitoreo periódico según su tipología:

Tipología	Monitoreo
Ejecución y administración de procesos Fraude externo Fallas tecnológicas Relaciones laborales Usuarios, productos y prácticas Daños a activos fijos/ eventos externos Seguridad de la información	Trimestral
Corrupción (Fraude interno)	Mensual

Ilustración 6. Tiempos para el desarrollo del Monitoreo
Fuente: Elaborado y adoptado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas por el Grupo de Planeación – Desarrollo Institucional de la DIGSA.

9.9 Seguimiento

Uno de los roles que reglamentariamente desarrolla por el Grupo se Seguimiento y Evaluación es el de “Evaluar la Gestión del Riesgo” como tercera línea de defensa, proporcionando a la Alta Dirección información relacionada con la efectividad del Sistema de Control Interno, basado en las actuaciones de la primera y segunda línea de defensa. Mediante el proceso de auditoría se verificará cómo opera la gestión del riesgo de la entidad, brindando información que permita a la primera línea tomar decisiones de carácter estratégico, proteger los recursos y minimizar riesgos que puedan afectar el cumplimiento de los objetivos.

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

De acuerdo a la identificación, clasificación, criticidad, nivel de impacto, Identificación de las Infraestructuras Críticas Cibernéticas (ICC) y la clasificación de la información de los activos de información de la Dirección General de Sanidad Militar realizado en la presente vigencia; se debe realizar el Plan de Tratamiento de Riesgos de los activos de información que fueron catalogados con nivel de criticidad alto en cada uno de los procesos de la DIGSA.

A continuación, se describen las actividades que se van a realizar en la vigencia 2022, así:

No.	Actividad	Responsables	Evidencia actividad	Fecha
1	Realizar el análisis, evaluación y tratamiento de riesgos de los activos de información que fueron catalogados con nivel de criticidad alto en cada uno de los procesos de la DIGSA; de acuerdo con la guía de Administración del Riesgo SSFM DIGSA	Subdirectores Coordinadores Líderes de Proceso	Mapa de Riesgos Institucional DIGSA	Enero-Junio
2.	Monitorear la efectividad de los controles existentes.	Gestor del Proceso	Monitoreo de riesgos plataforma Suite Visión Empresarial-SVE	Trimestral
3.	Seguimiento a la efectividad de los controles	Grupo Seguimiento y Evaluación	Observación o novedad al control por parte del Grupo de Seguimiento y Evaluación.	Trimestral

Ilustración 7. Actividades 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[2].

12. Bibliografía

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, versión 4 de 2018. Bogotá.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la Administración del Riesgo y el diseño de Controles en entidades Públicas, versión 5 de 2020. 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.

Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC. Norma Técnica Colombiana NTC ISO 31000:2018. Gestión del Riesgo. Principios y Directrices. Bogotá D.C.

[2] 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”.