PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2025

TABLA DE CONTENIDO

OBJETIVO

Establecer un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, alineado a las normativas vigentes, que permita gestionar eficazmente los riesgos de los activos críticos. Este plan servirá como guía para minimizar la probabilidad e impacto de amenazas, asignando roles claros y promoviendo una cultura de seguridad digital en la entidad.

OBJETIVO ESPECIFICOS:

- Evaluar y analizar los riesgos de seguridad digital de los activos de información para garantizar la protección y continuidad de los procesos que sustentan la misión de la entidad.
- Identificar las amenazas e impactos en seguridad digital asociados a los procesos clave de la entidad, priorizando aquellos que afectan la confidencialidad, integridad y disponibilidad de la información.
- Implementar controles de seguridad efectivos que gestionen los riesgos identificados y apoyen la toma de decisiones informada sobre el riesgo residual.
- Establecer un plan de tratamiento para el riesgo residual, orientado a minimizar su impacto y asegurar una gestión proactiva de los riesgos de seguridad de la información.

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se aplicará a todos los activos de información de la entidad, incluyendo procesos, servicios, sistemas de información, así como a los servidores públicos, terceros y partes interesadas que gestionen o utilicen información y servicios tecnológicos en el marco de sus funciones. La gestión de riesgos se realizará conforme a las normativas vigentes, alineada con buenas prácticas y metodologías recomendadas, tales como las pautas de la ISO 27001, y estará orientada a integrar prácticas de seguridad digital en los procesos de la entidad para la prevención de incidentes y la toma de decisiones informadas. El alcance incluye la gestión integral de los riesgos clasificados en niveles moderado, alto y extremo, con un enfoque de mejora continua para proteger la confidencialidad, integridad y disponibilidad de la información en cumplimiento del marco normativo aplicable.

NORMATIVIDAD

Se mencionan algunos de los marcos legales y requisitos técnicos que tienen relación con la política de seguridad y privacidad de la información, seguridad digital y continuidad del negocio, que ayudan a la debida implementación y que se podrían cumplir en algunos de los apartados:

Marco legal

1. **Leyes**

- Constitución Política de Colombia (1991) – Artículo 15: “Todas las personas tienen derecho a su intimidad personal y familiar ya su buen nombre. Así mismo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.”
- Ley 527 de 1999 – "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales; se establecen las entidades de certificación y se dictan otras disposiciones".
- Ley 1474 de 2011 – *"Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública".
- Ley 1581 de 2012 – "Por la cual se dictan disposiciones generales para la protección de datos personales".
- El artículo 15 de la Constitución reconoce el derecho fundamental a la intimidad personal y familiar, así como al buen nombre. También garantiza el derecho a conocer, actualizar y rectificar información personal. Aunque hace referencia al hábeas data, no lo menciona expresamente como un derecho fundamental bajo dicha denominación, Ley 1581 de 2012 (Ley de Protección de Datos Personales).

2. **Decretos**

- Decreto 103 de 2015, Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
- Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector de las TIC)
- Decreto 1494 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- Decreto 612 de 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
- Decreto 1008 de 2018 (Política de Gobierno Digital)

3. **Resoluciones**

- Resolución 500 de marzo 10 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.

4. **Normas Técnicas**

   - NTC / ISO 27001:2013, Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.
   - NTC/ISO 31000:2009, Gestión del Riesgo. Principios y directrices.

5. **Políticas**

   - CONPES 3854 de 2016, Política Nacional de Seguridad Digital.

GLOSARIO

- **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.
- **Activo de información**: Conocimiento o datos que son de valor para la entidad.
- **Acceso a la información pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados (Ley 1712 de 2014, art 4).
- **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).
- **Amenaza**: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. 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 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).
- **Confidencialidad**: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Control**: Medida que permite reducir o mitigar un riesgo. Entiéndase por las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida.
- **Disponibilidad**: Propiedad de ser accesible y utilizable a demanda por una entidad.
- Evaluación del riesgo: Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).
- **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.

- **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).
- **Identificación del riesgo**: Se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, 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.
- **Integridad**: Propiedad de exactitud y completitud.
- **Impacto**: Son las consecuencias que genera un riesgo una vez se materialice.
- **Modelo de Seguridad y Privacidad de la Información (MSPI)**: Imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades.
- **Probabilidad**: Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual**: Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.
- **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 constitucional y los intereses nacionales. Incluye aspectos del ambiente físico, digital y las personas.
- **Seguridad de la información**: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, puede involucrar otras propiedades como como: autenticidad, trazabilidad, no repudio y fiabilidad.
- **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. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Tratamiento del riesgo**: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.
- **Valoración de riesgos**: Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).
- **Vulnerabilidad**: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

PROFUNDIZACIÓN DEL PLAN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se desarrolla conforme a las cinco fases establecidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información, el cual

es un habilitador fundamental de la Política de Gobierno Digital del Gobierno Nacional, impulsada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

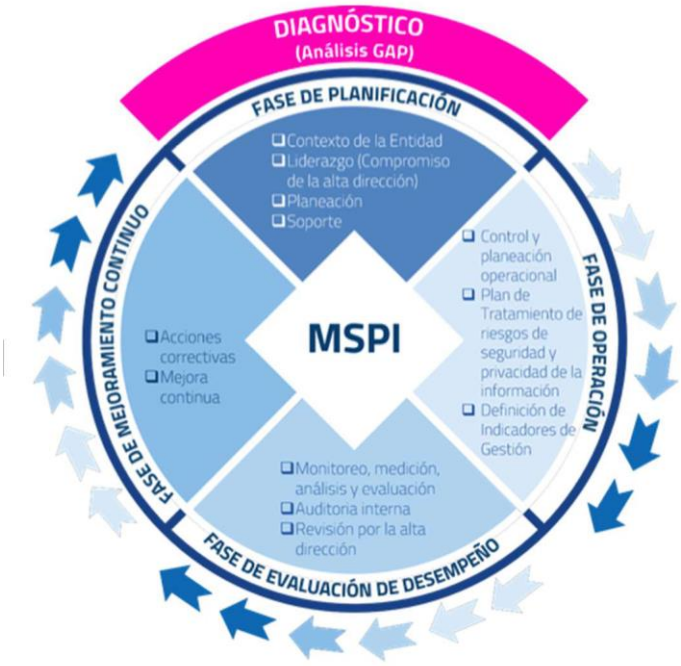

Imagen 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

I. Fase Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad de la Información.

II. Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

III. Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

IV. Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

V. Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

Alineación del Ciclo de Operación con la Norma ISO 27001:2013

Si bien la norma ISO 27001:2013 no especifica un modelo de mejora continua (PHVA) como requisito para estructurar los procesos de seguridad y privacidad de la información, es posible alinear la nueva estructura de

esta versión con el ciclo de mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) de la siguiente manera:

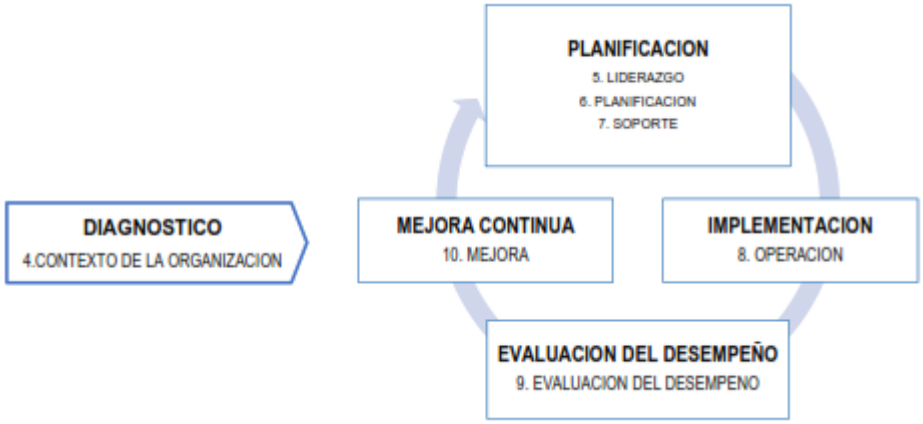

Figura 2: Norma ISO 27001:2013 alineado al ciclo de mejora continua

A continuación, se muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Fase	Capitulo ISO 27001:2013
Diagnostico	4. Contexto de la Organización
Planificación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

- Fase diagnostico en la norma ISO 27001:2013: En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del modelo de seguridad de la información.

- Fase planeación en la norma ISO 27001:2013: En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos respecto a la seguridad y privacidad de la Información y entre otros aspectos, la necesidad de que se establezca una política de seguridad de la información adecuada al propósito de la entidad y asegure la asignación de los recursos para la seguridad de la información y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen. En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento. En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua aplicable al Modelo de Seguridad y Privacidad de la Información (MSPI).

- Fase implementación en la norma ISO 27001:2013: En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- Fase evaluación del desempeño en la norma ISO 27001:2013: En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

Fase I: Diagnostico

El objetivo de esta fase es el de identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Figura 2: Fase de diagnóstico del plan de tratamiento de riesgos de seguridad y privacidad de la información.

Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la seguridad y privacidad de la información al interior de la entidad.	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información.

	Diagnostico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013. Valoración estado actual de la seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad.	Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad y privacidad de la información.
- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

Fase II: Planificación

El objetivo de esta fase es definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad y privacidad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas por la entidad.

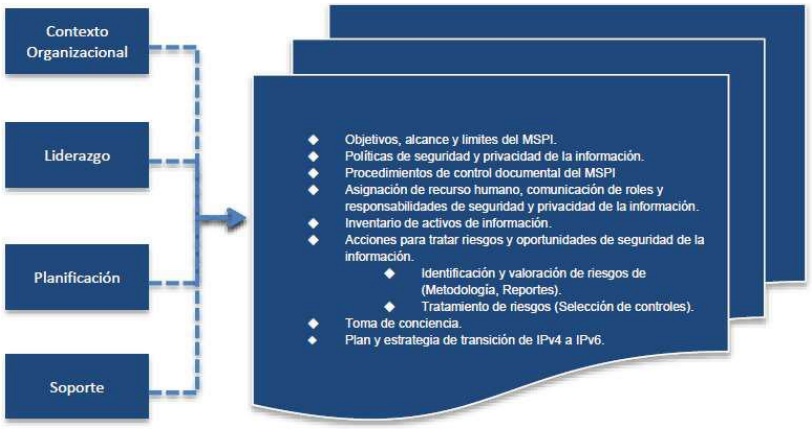

Figura 3: Fase de planificación del plan de tratamiento de riesgos de seguridad y privacidad de la información.

Metas	Actividades \ Instrumentos \ Resultados
Realizar un análisis de Contexto y factores externos e internos de la	Realizar un análisis de contexto de la entidad entorno a la seguridad de

entidad en torno a la seguridad de la información.	la información teniendo en cuenta el capítulo 4. Contexto de la organización de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Plan de tratamiento de riesgos de seguridad y privacidad de la información.
Definir el alcance del Plan de tratamiento de riesgos de seguridad y privacidad de la información de la entidad.	Definir el alcance del Plan de tratamiento de riesgos de seguridad y privacidad de la información de la entidad aprobado y socializado al interior de la entidad.
Definir roles, responsables y funciones de seguridad y privacidad de la información.	Adicionar las funciones de seguridad de la información a toda la entidad y formalizarlas. Establecer el rol de Oficial de seguridad de la información. Definir un marco de gestión que contemple roles y responsabilidades para la implementación, administración, operación y gestión de la seguridad de la información en la entidad. Definir la estructura organizacional de la entidad que contendrá los roles y responsabilidad pertinentes a la seguridad y privacidad de la información.
Definir la metodología de riesgos de seguridad de la información	Definir metodología de valoración de riesgos de seguridad. Integrar la metodología definida con la metodología de riegos operativos de la entidad.
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Elaborar los documentos de operación del Plan de tratamiento de riesgos de seguridad y privacidad de la información, tales como: ● Procedimiento y/o guía de identificación y clasificación de activos de información. ● Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI. ● Procedimiento para control de documentos. ● Procedimiento para auditoría interna. ● Procedimiento para medidas correctivas. ● Procedimiento para la gestión de eventos e incidentes de seguridad y privacidad de la información. ● Procedimiento para la gestión de vulnerabilidades de seguridad y privacidad de la información. ● Entre otros.
Identificar y valorar activos de información.	Realizar la identificación y valoración de los activos de información de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del Plan de tratamiento de riesgos de seguridad y privacidad de la información. Documentar el inventario de los activos de información de la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad.	Realizar la identificación y valoración de los riesgos transversales de seguridad y privacidad de la información y definir los respectivos planes

	de tratamiento. Realizar la valoración de riesgos de seguridad y privacidad de la información. Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración.
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.	Elaborar plan anual de capacitación y sensibilización del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

Fase III: Implementación

El objetivo de esta fase es llevar a cabo la implementación de la fase de planificación, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Plan de tratamiento de riesgos de seguridad y privacidad de la información de la entidad.

Figura 4: Fase de implementación del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

Metas	Actividades \ Instrumentos \ Resultados
Establecer el Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Implementar el Plan de tratamiento de riesgos de seguridad y privacidad de la información el cual debe ser revisado y aprobado.
Implementar procedimiento de gestión de eventos e incidentes de seguridad y privacidad de la información.	Implementar el procedimiento y los mecanismos para la gestión de los eventos e incidentes de seguridad y privacidad de la información.
Implementar procedimiento de gestión de vulnerabilidades.	Implementar el procedimiento y los mecanismos para la gestión de vulnerabilidades seguridad y privacidad de la información.
Ejecutar plan de capacitación y sensibilización de seguridad.	Ejecutar el plan anual de capacitación, socialización y sensibilización de seguridad y privacidad de la información.
Ejecutar pruebas anuales de vulnerabilidades e intrusión.	Ejecutar el plan anual de pruebas vulnerabilidades e intrusión con el objetivo de identificar el nivel de protección de los activos de información

	de la entidad.
Ejecutar pruebas de Ethical Hacking.	Ejecutar pruebas anuales de Ethical Hacking orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan a comprometer activos críticos de la entidad y con esto generar interrupción en los servicios, afectar la continuidad del negocio y/o acceder de forma no autorizada a la información sensible o clasificada de la entidad o de carácter personal de los trabajadores o terceros que laboren para la entidad.
Ejecutar pruebas de Ingeniera Social.	Ejecutar pruebas anuales de ingeniería social orientadas a verificar aspectos como: (i) los protocoles internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y de sus empleados.

Fase IV: Evaluación de desempeño

El objetivo de esta fase es evaluar el desempeño y la eficacia del Plan de tratamiento de riesgos de seguridad y privacidad de la información, a través de instrumentos que permita determinar la efectividad de la implantación.

Figura 5: Fase de evaluación del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

Metas	Actividades \ Instrumentos \ Resultados
Ejecución de auditorías de seguridad y privacidad de la información.	Ejecución de auditorías del Plan de tratamiento de riesgos de seguridad y privacidad de la información y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado. Las auditorías internas se deberán llevar a cabo para la revisión del Plan de tratamiento de riesgos de seguridad y privacidad de la información implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos cumplan con los requisitos establecidos en la norma ISO 27002:2013.
Plan de seguimiento, evaluación y análisis de Plan de tratamiento de	Elaboración documento con el plan de seguimiento, evaluación y

riesgos de seguridad y privacidad de la información.	análisis del Plan de tratamiento de riesgos de seguridad y privacidad de la información revisado y aprobado.

Fase V: Mejora continua

El objetivo de esta fase es consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para la seguridad y privacidad de la información de la entidad.

Figura 6: Fase de mejora continua del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

Metas	Actividades \ Instrumentos \ Resultados
Diseñar plan de mejoramiento.	Diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el Plan de tratamiento de riesgos de seguridad y privacidad de la información.

MONITOREO, SEGUIMIENTO Y EVALUACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración interactiva de los riesgos de seguridad y privacidad 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.

El monitoreo, seguimiento y evaluación de los riesgos de seguridad y privacidad de la información en las entidades es una responsabilidad compartida que generalmente involucra a varios roles clave. Según las normativas internacionales y locales (como ISO 27001, ISO 27005, y las políticas nacionales de seguridad digital), estos roles incluyen:

1. **Alta Dirección:**
    - Responsable de supervisar y garantizar la implementación adecuada del sistema de gestión de seguridad y privacidad de la información.
    - Aprueba recursos y estrategias necesarias para gestionar los riesgos.
2. **Oficial de Seguridad de la Información (CISO):**
    - Lidera las actividades de identificación, análisis, evaluación, tratamiento y monitoreo de riesgos.
    - Garantiza la alineación con las normativas y estándares aplicables.
3. **Comités de Seguridad de la Información:**
    - Supervisan la implementación del sistema de gestión y los planes de tratamiento de riesgos.
    - Evalúan la eficacia de las medidas adoptadas y proponen mejoras.
4. **Jefes de Área o Responsables de Procesos:**
    - Gestionan los riesgos específicos de sus áreas o procesos.
    - Aseguran el cumplimiento de las políticas y controles establecidos.
5. **Encargados de Tecnologías de la Información (TI):**
    - Implementan medidas técnicas para mitigar riesgos en la infraestructura tecnológica.
    - Realizan el monitoreo continuo de sistemas y redes.
6. **Auditores Internos y Externos:**
    - Verifican la conformidad del sistema de gestión de riesgos con las normativas y estándares.
    - Evalúan la eficacia de las medidas de seguridad implementadas.
7. **Usuarios Finales:**

    Cumplen con las políticas de seguridad de la información y reportan incidentes o vulnerabilidades.

En Colombia, entidades públicas se rigen también por normativas como el Decreto 1008 de 2018 y la Ley 1581 de 2012, que establecen responsabilidades específicas para los responsables del tratamiento de datos y encargados de seguridad de la información.

Tabla 1Probabilidad de riesgo

PROBABILIDAD DE RIESGOS			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento.	Al menos una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla 2 Impacto del Riesgo

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimo sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.

5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Riesgo inherente: Criticidad=probabilidad*Impacto

Tabla 3Matriz de calificación, evaluación y respuesta a los riesgos.

Fuente: Guía de Riesgos DAFP

100% **Muy alta**	*Tolerancia Alta 21*	*Tolerancia Alta 22*	*Tolerancia Alta 23*	*Tolerancia Alta 24*	*Capacidad Extrema 25*
80% **Alta**	*Tolerancia Moderada 16*	*Tolerancia Moderada 17*	*Tolerancia Alta 18*	*Tolerancia Alta 19*	*Capacidad Extrema 20*
60% **Media**	*Tolerancia Moderada 11*	*Tolerancia Moderada 12*	*Tolerancia Moderada 13*	*Tolerancia Alta 14*	*Capacidad Extrema 15*
40% **Baja**	*Aceptación Baja 6*	*Tolerancia Moderada 7*	*Tolerancia Moderada 8*	*Tolerancia Alta 9*	*Capacidad Extrema 10*
20% **Muy Baja**	*Aceptación Baja 1*	*Aceptación Baja 2*	*Tolerancia Moderada 3*	*Tolerancia Alta 4*	*Capacidad Extrema 5*
	20% **Leve**	40% **Menor**	60% **Moderado**	80% **Mayor**	100% **Catastrófico**

RECURSOS

De acuerdo a la Política Seguridad y Privacidad De La Información, Seguridad Digital y Continuidad Del Negocio, se desarrolla el Plan de tratamiento de riesgos de seguridad y privacidad de la información, el Club Militar dispone de los siguientes recursos:

- Humanos: El Grupo de Gestión TIC dispone de personal responsable de la coordinación e implementación de herramientas, sistemas, políticas, procedimientos, prácticas o mecanismos dinámicos y seguros para el tratamiento de los riesgos. Asimismo, se dispone del apoyo de los demás procesos que intervienen en el desarrollo del plan.

- Técnicos: Se dispone documentos guías para la administración del riesgo, políticas de administración del riesgo y seguridad y privacidad de la información, mapas de riesgos para el registro y evidencia del proceso por la Entidad.

- Físicos: Se cuenta con la infraestructura tecnológica y física para el desarrollo de actividades como socializaciones, transferencia de conocimientos, comunicación del riesgo, seguimiento y evaluación a la gestión del riesgo.
- Financieros: El Club Militar dispone de recursos financieros para la implementación de las acciones que requieran la contratación de servicios o la compra de bienes, los cuales son descritos en los planes de compras anuales.

PRESUPUESTO:

El Club Militar demuestra su compromiso frente a la seguridad de la información, mediante la asignación de presupuesto o recursos financieros para la implementación del Plan de tratamiento de riesgos de seguridad y privacidad de la información, El ítem asignado es el siguiente 078 SERVICIOS DE PRUEBAS ETHICAL HACKING PARA LOS SERVIDORES DEL CLUB MILITAR

CRONOGRAMA DE LAS ACTIVIDADES

N°	Descripción	Evidencia	Responsable	Inicio de la Actividad	Termino de la Actividad
1	Identificar y clasificar los activos de información, incluyendo datos sensibles y recursos tecnológicos.	Actualización del inventario de activos de información	Grupo Gestión Tic	01-01-2025	31-03-2025
2	Identificar posibles amenazas externas e internas que puedan afectar la seguridad de la información	Informe de alertas por posible contenido malicioso	Grupo Gestión Tic	01 - 01 - 2025 01 - 04 - 2025 01 - 07 - 2025 01 - 10 - 2025	31 - 03 - 2025 31 - 06- 2025 31 - 09 - 2025 31 – 12 - 2025
3	Revisión y seguimiento a los registros de logs de seguridad de la información	Hoja de Vida del indicador de seguridad informática	Grupo Gestión Tic	01 - 01 – 2025 01 - 04 - 2025 01 - 07 - 2025 01 - 10 - 2025	31 - 03 - 2025 31 - 06- 2025 31 - 09 - 2025 31 – 12 - 2025
4	Monitoreo y seguimiento de incidentes de seguridad	Informe de Riesgos	Grupo Gestión Tic	01 - 01 - 2025 01 - 04 - 2025 01 - 07 - 2025 01 - 10 - 2025	31 - 03 - 2025 31 - 06- 2025 31 - 09 - 2025 31 – 12 - 2025

5	Auditorias y evaluaciones internas de seguridad	Informes de Auditoría Interna y Externa Informe de Resultados de Evaluaciones de Riesgos	Oficina de Control Interno	01 - 01 - 2025 01 – 07 - 2025	31 - 06 - 2025 31 – 12 - 2025
6	Sensibilización y socialización sobre temas de seguridad	Actas de reunión y/o evidencia de envió de correos sobre la importancia de la seguridad de la información y/o campañas del papel tapiz en los equipos de computo de las tres sedes del Club Militar	Grupo Gestión Tic	01 - 01 - 2025 01 - 04 - 2025 01 - 07 - 2025 01 - 10 - 2025	31 - 03 - 2025 31 - 06- 2025 31 - 09 - 2025 31 – 12 - 2025
7	Revisar y verificar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación identificados.	Informe de Pruebas de Ethical Hacking	Grupo Gestión Tic	01-10-2025	30-12-2025

ROLES Y RESPONSABILIDADES

1. Alta Dirección

- Aprobar el plan de tratamiento de riesgos de seguridad de la información y los recursos necesarios para su implementación.
- Revisar periódicamente los informes de seguimiento del plan y realizar ajustes en función de los resultados.
- Definir las prioridades estratégicas de gestión de riesgos de acuerdo con los objetivos de la entidad.
- Fomentar una cultura de seguridad en toda la organización mediante la comunicación de la importancia de la seguridad de la información y el cumplimiento de normativas.

2. Oficina de control Interno

- Evaluar el cumplimiento de las políticas de seguridad de la información y el plan de tratamiento de riesgos.
- Realizar auditorías periódicas para asegurar la efectividad de los controles de seguridad implementados.

- Informar sobre incumplimientos y proponer acciones de mejora.
- Verificar que se documente adecuadamente el monitoreo y seguimiento de incidentes y riesgos materializados.

3. Oficial de Seguridad de la Información (CISO)

- Coordinar y supervisar todas las actividades del plan de tratamiento de riesgos.
- Identificar y evaluar los riesgos de seguridad de la información, en colaboración con las áreas responsables.
- Asegurar que se cumpla con las normativas y políticas de seguridad de la información.
- Comunicar y reportar el estado del tratamiento de riesgos a la alta dirección y a los comités correspondientes.
- Implementar y administrar los controles técnicos de seguridad (firewalls, antivirus, gestión de accesos, etc.).
- Detectar y responder a incidentes de seguridad de la información.
- Asegurar la continuidad operativa y la integridad de los activos de información.

4. Líderes de Proceso o Responsables de Áreas

- Identificar los activos de información y sus riesgos asociados en sus respectivas áreas.
- Informar sobre incidentes y riesgos emergentes al Oficial de Seguridad de la Información.
- Participar en las charlas reuniones y/o capacitaciones junto a su personal a cargo sobre seguridad y privacidad de la información.
- Verificar que todos los colaboradores del área cumplan y respeten las políticas de seguridad y privacidad de la información establecidas por la entidad

DOCUMENTOS DE APOYO

- POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- INSTRUCTIVO GESTION INCIDENTES SEGURIDAD Y PRIVACIDAD INFORMACION

ANEXOS

- N/A

CONTROL DE CAMBIOS

VERSIÓN	FECHA DEL CAMBIO	DESCRIPCIÓN DE LA ACTUALIZACIÓN
1	10-08-2023	Creación de documento.
2	31-01-2024	Actualización de actividades vigencia 2024.
3	30-01-2025	Actualización de actividades, alineado al Modelo de Seguridad y Privacidad de la Información

VALIDACIÓN DE FIRMAS

	NOMBRE	CARGO
ELABORO:	ASSD. Santiago Sanmiguel	ASSD Grupo de Gestión TIC
REVISO:	Yudyett Astrid Pulido Guevara	Sistemas Integrados de Gestión – OAP.
APROBO:	Javier Parra Pinzón	Coordinador Grupo Gestión TIC
	TC (RA) (E) Juan Carlos Arenas Fonseca	Jefe Oficina De Planeación.
	Dr. Edgardo Muñoz Chegwin	Jefe Oficina Asesora Jurídica.
	TC (RA) (E) Juan Carlos Arenas Fonseca	Subdirector General del Club Militar.
FIRMANTE:	BG (RA) José Henry Pinto Rodríguez	Director General del Club Militar.

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL-03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2025

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20250130-093124-546e44-74860955
Estado: Finalizado
Creación: 2025-01-30 09:31:24
Finalización: 2025-01-31 07:58:35

Escanee el código para verificación

Aprobación: Jefe Oficina De Planeación.

JUAN CARLOS ARENAS
79557085
jcarenas@clubmilitar.gov.co

Aprobación: Coordinador Grupo Gestión TIC

Javier Parra Pinzon
1012377884
jparra@clubmilitar.gov.co
ASSD
Club Militar

Revisión: Sistemas Integrados de Gestión ? OAP.

Yudyett Pulido
52915896
yapulido@clubmilitar.gov.co

Elaboración: ASSD Grupo de Gestión TIC

Santiago Andres Sanmiguel Murillo
1000252838
sasanmiguel@clubmilitar.gov.co
ASSD
Club Militar

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL-03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2025

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20250130-093124-546e44-74860955
Estado: Finalizado
Creación: 2025-01-30 09:31:24
Finalización: 2025-01-31 07:58:35

Escanee el código para verificación

Firma: BG (RA) José Henry Pinto Rodríguez

Brigadier General (RA) José Henry Pinto Rodriguez
16278442
asistentedireccion@clubmilitar.gov.co
Director General
Club Militar

Aprobación: Subdirector General del Club Militar.

JUAN CARLOS ARENAS
79557085
jcarenas@clubmilitar.gov.co

Aprobación: Jefe Oficina Asesora Jurídica.

Edgardo Muñoz Chegwin
79408386
emunoz@clubmilitar.gov.co
Jefe Oficina Asesora Jurídica
CLUB MILITAR

REPORTE DE TRAZABILIDAD

CM-GTI-PL-03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2025

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20250130-093124-546e44-74860955
Creación: 2025-01-30 09:31:24
Estado: Finalizado
Finalización: 2025-01-31 07:58:35

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Santiago Andres Sanmiguel Murillo sasanmiguel@clubmilitar.gov.co ASSD Club Militar	Aprobado	Env.: 2025-01-30 09:31:25 Lec.: 2025-01-30 09:35:39 Res.: 2025-01-30 09:36:04 IP Res.: 200.91.222.50
Revisión	Yudyett Pulido yapulido@clubmilitar.gov.co	Aprobado	Env.: 2025-01-30 09:36:04 Lec.: 2025-01-30 09:43:30 Res.: 2025-01-30 09:44:13 IP Res.: 200.91.222.50
Aprobación	Javier Parra Pinzon jparra@clubmilitar.gov.co ASSD Club Militar	Aprobado	Env.: 2025-01-30 09:44:13 Lec.: 2025-01-30 09:45:40 Res.: 2025-01-30 09:45:53 IP Res.: 186.31.153.176
Aprobación	JUAN CARLOS ARENAS jcarenas@clubmilitar.gov.co	Aprobado	Env.: 2025-01-30 09:45:53 Lec.: 2025-01-30 12:23:23 Res.: 2025-01-30 12:23:31 IP Res.: 200.91.249.34
Aprobación	Edgardo Muñoz Chegwin emunoz@clubmilitar.gov.co Jefe Oficina Asesora Jurídica CLUB MILITAR	Aprobado	Env.: 2025-01-30 12:23:31 Lec.: 2025-01-30 12:24:44 Res.: 2025-01-30 13:18:02 IP Res.: 200.91.222.50
Aprobación	JUAN CARLOS ARENAS jcarenas@clubmilitar.gov.co	Aprobado	Env.: 2025-01-30 13:18:02 Lec.: 2025-01-30 14:18:05 Res.: 2025-01-30 14:18:15 IP Res.: 200.91.249.34
Firma	Brigadier General (RA) José Henry Pin asistentedireccion@clubmilitar.gov.co Director General Club Militar	Aprobado	Env.: 2025-01-30 14:18:15 Lec.: 2025-01-30 14:53:53 Res.: 2025-01-31 07:58:35 IP Res.: 190.109.17.26