# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

**TABLA DE CONTENIDO**

## OBJETIVO

Establecer un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, alineado a las normativas vigentes y al Modelo de Seguridad y Privacidad de la Información (MSPI), 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 ESPECÍFICOS:

- Evaluar el panorama de riesgos: Actualizar el mapa de riesgos de seguridad digital, identificando nuevas amenazas emergentes y vulnerabilidades en la infraestructura tecnológica institucional.
- Implementar controles técnicos y administrativos efectivos, incluyendo pruebas especializadas de seguridad (Ethical Hacking), para mitigar los riesgos clasificados como moderados, altos y extremos
- Ejecutar estrategias de sensibilización que minimicen los riesgos asociados al factor humano, como la ingeniería social.
- Monitorear la eficacia de los controles mediante indicadores de gestión y auditorías internas, garantizando la toma de decisiones basada en datos.

## ALCANCE

Este plan cubre la totalidad de los activos de información del Club Militar (físicos y digitales), los sistemas de información, la infraestructura tecnológica y el talento humano (servidores públicos y contratistas). Su aplicación es transversal a todas las sedes y procesos de la entidad, enfocándose prioritariamente en el tratamiento de riesgos residuales que superen los niveles de tolerancia aceptados por la institución.

## 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**

- **Leyes**
- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Ley 1581 de 2012 (Ley de Protección de Datos Personales)
- Ley 527 de 1999 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.

- Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional)
- Ley 1474 de 2011, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
- **Decretos**
- 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)
- 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
- **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.
- **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.
- **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).

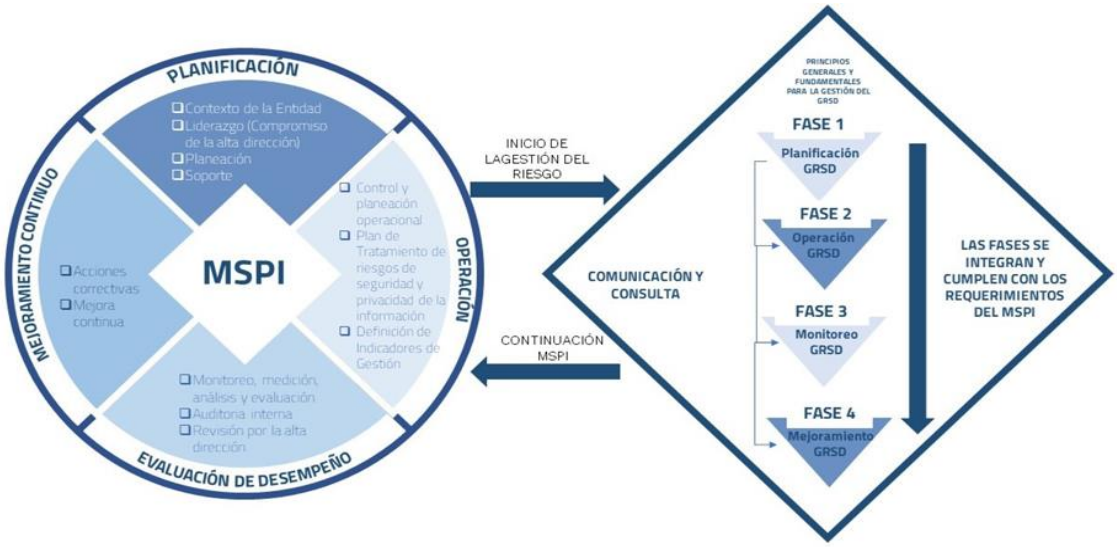



Imagen 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

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

2. 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.

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

4. 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.

5. 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 27001:2022

El Modelo de Seguridad y Privacidad de la Información (MSPI) del Club Militar se fundamenta en la norma ISO/IEC 27001:2022, la cual integra de manera intrínseca el ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar). Esta alineación permite estructurar los procesos de seguridad y privacidad a través de las 5 fases operativas definidas por el MinTIC (Diagnóstico, Planificación, Operación, Evaluación de Desempeño y Mejoramiento Continuo), garantizando la gestión de los 93 controles de seguridad vigentes.

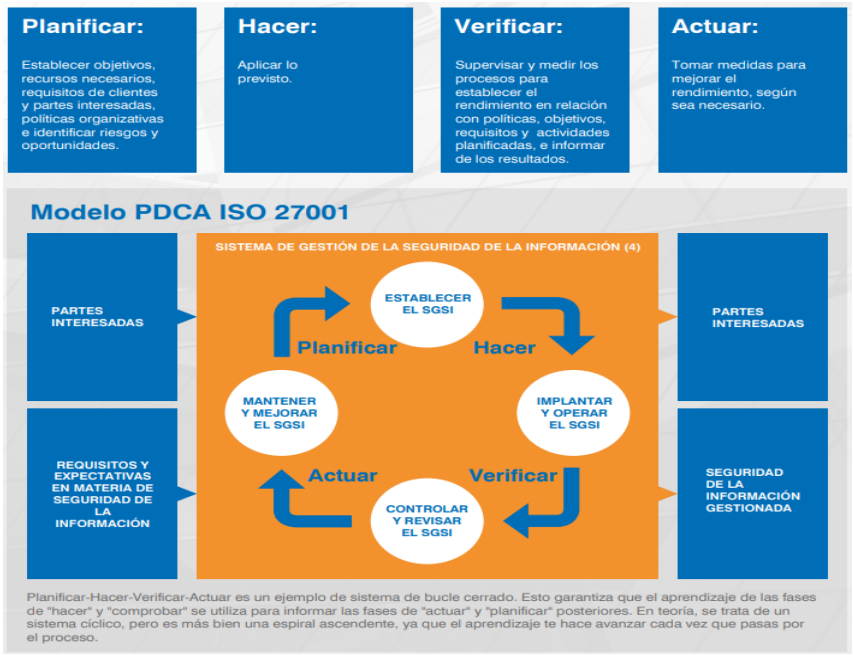



Figura 1: Norma ISO 27001:2022 alineado al ciclo de mejora continua

A continuación, se muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Planificación, Hacer, Verificar y Actuar) y la estructura de capítulos y numerales de la norma ISO 27001:2022:

| Fase (Ciclo PHVA / PDCA) | Capítulo ISO/IEC 27001:2022 | Descripción Ajustada |
|---|---|---|
| Planificación (Plan) | Cláusulas 4, 5, 6 y 7 | Establecer el SGSI: contexto de la organización, liderazgo, planificación, evaluación de riesgos y recursos necesarios. |
| Hacer (Do) | Cláusula 8 | Implantar y operar el SGSI: implementación de los controles, operación de procesos y ejecución del tratamiento de riesgos. |
| Verificar (Check) | Cláusula 9 | Controlar y revisar el SGSI: monitoreo, medición, análisis, auditorías internas y revisión por la dirección. |

| | | |
|---|---|---|
| Actuar (Act) | Cláusula 10 | Mantener y mejorar el SGSI: acciones correctivas y mejoras continuas del sistema. |

**FASE I: PLANIFICACIÓN**

La fase de Planificación consiste en establecer las bases del Sistema de Gestión de Seguridad de la Información (SGSI), definiendo contexto, líderes, lineamientos, objetivos, riesgos y recursos.

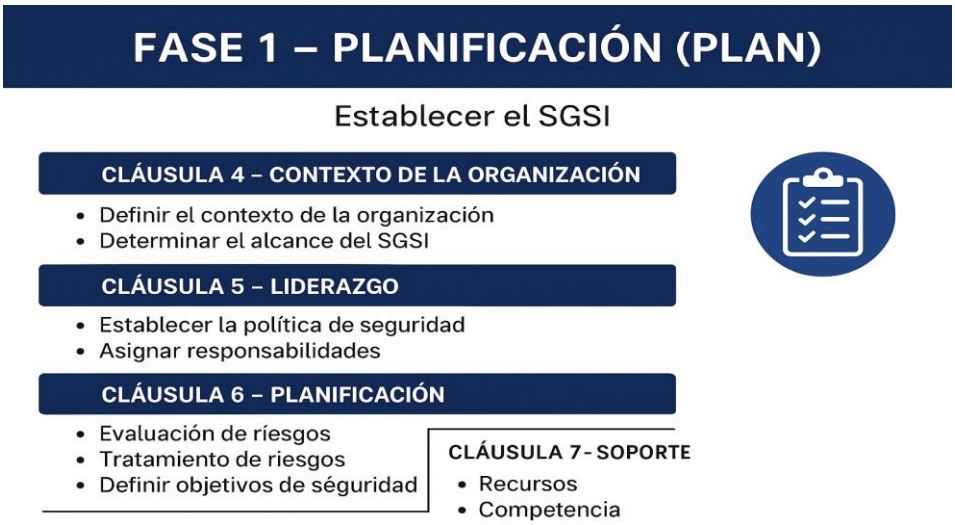



Figura 2: Fase de planificación del plan de tratamiento de riesgos de seguridad y privacidad de la información.

| Meta | Actividades / Instrumentos | Resultados |
|---|---|---|
| Determinar el estado actual de la seguridad y privacidad de la información al interior de la entidad. | • Realizar un diagnóstico integral del sistema de gestión de seguridad de la información (SGSI) frente a los requisitos de la ISO/IEC 27001:2022. • Evaluación del grado de cumplimiento frente a los nuevos 93 controles de la ISO/IEC 27001:2022, organizados en los dominios: Organizacional, Personas, Físico y Tecnológico. • Aplicación del Instrumento de Evaluación MSPI – MINTIC para medir el estado de la seguridad y privacidad en la entidad. | • Informe de diagnóstico del estado actual del SGSI. • Nivel de cumplimiento de los requisitos de la ISO/IEC 27001:2022. • Valoración institucional según la metodología MSPI del MINTIC. |
| Identificar el nivel de madurez de la seguridad y privacidad de la información. | • Evaluación del nivel de madurez del SGSI teniendo en cuenta los atributos de los controles de ISO/IEC 27001:2022 (cibernético, operativo, físico, organizacional y de personas). • Aplicación de modelos de madurez basados en MSPI e ISO/IEC 27001:2022. | • Informe de nivel de madurez del SGSI con brechas y necesidades de mejora priorizadas. |
| Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación. | • Ejecución de pruebas de vulnerabilidades sobre infraestructura tecnológica, aplicaciones y redes, alineadas con los controles del dominio tecnológico de ISO/IEC 27001:2022. • Identificación de debilidades en procesos, roles, accesos, documentación y prácticas operativas. | • Informe detallado de vulnerabilidades técnicas y administrativas. • Recomendaciones iniciales y planes de mitigación alineados con la norma ISO/IEC 27001:2022. |

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 27001:2022.

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: HACER**

La fase de Hacer consiste en implementar y operar el SGSI mediante la ejecución de los controles y acciones planificadas, asegurando que los riesgos identificados sean tratados según el plan de tratamiento de riesgos.


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

| Metas | Actividades / Instrumentos | Resultados |
|---|---|---|
| Implementar los procedimientos, controles o estrategias establecidos | • Ejecutar las actividades definidas en el SGSI conforme a ISO 27001:2022<br>• Realizar análisis de contexto para identificar cuestiones internas y externas.<br>• Aplicar los controles definidos en el Anexo A:2022 en función del plan de tratamiento de riesgos. | • Controles implementados y funcionales.<br>• Contexto institucional documentado y actualizado.<br>• Evidencias de implementación registradas. |
| Garantizar que los equipos responsables comprendan y apliquen las tareas asignadas | • Definir y comunicar el alcance del SGSI y del Plan de Tratamiento<br>• Socializar roles y responsabilidades | • Alcance aprobado y divulgado.<br>• Equipos responsables capacitados y alineados con sus funciones. |

| | | |
|---|---|---|
| Definir roles, responsables y funciones de seguridad y privacidad | • Formalizar roles del Oficial de Seguridad de la Información y responsables de privacidad<br>• Actualizar estructura organizacional con roles de seguridad, privacidad y continuidad.<br>• Establecer marco de gestión alineado | • Estructura organizacional definida.<br>• Roles formalizados mediante resoluciones o documentos oficiales. |
| Definir la metodología de riesgos de seguridad y privacidad | • Diseñar la metodología de valoración de riesgos<br>• Integrar la metodología con esquemas de riesgo institucional existentes (riesgo operativo, estratégico, tecnológico). | • Metodología de riesgos aprobada.<br>• Modelo de riesgos integrado a la organización. |
| Elaborar documentación operativa del Plan de Tratamiento | Elaborar o actualizar documentos conforme ISO 27001:2022:<br>• Procedimiento de clasificación de activos<br>• Procedimientos de continuidad •<br>Procedimiento de control documental<br>• Procedimiento de auditoría interna<br>• Procedimiento de acciones correctivas<br>• Procedimiento de gestión de incidentes<br>• Procedimiento de vulnerabilidades | • Procedimientos aprobados y operativos. • Documentación actualizada y controlada según |
| Identificar y valorar activos de información | • Identificación y clasificación de activos<br>• Valoración de criticidad basada en C-I-D.<br>• Actualización del inventario de activos conforme al alcance. | • Inventario actualizado.<br>• Activos valorados según criterios definidos. |
| Identificar, valorar y tratar los riesgos de seguridad y privacidad | • Ejecutar identificación y valoración de riesgos conforme a la metodología definida. • Documentar riesgos, controles existentes, brechas y niveles de riesgo. • Formular los planes de tratamiento con responsables, plazos y controles | • Matriz de riesgos actualizada.<br>• Planes de tratamiento aprobados y en ejecución.<br>• Decisiones de riesgo justificadas (aceptar, reducir, transferir, evitar). |
| Establecer plan de capacitación, comunicación y sensibilización | • Elaborar plan anual de capacitación y sensibilización • Desarrollar actividades, campañas y contenidos dirigidos a todo el personal. | • Personal sensibilizado y capacitado.<br>• Evidencias documentadas de cumplimiento del plan anual. |

**FASE III: VERIFICAR**

Evaluar la eficacia de la implementación, medir resultados, identificar brechas y validar el cumplimiento del SGSI y del Plan de Tratamiento de Riesgos.

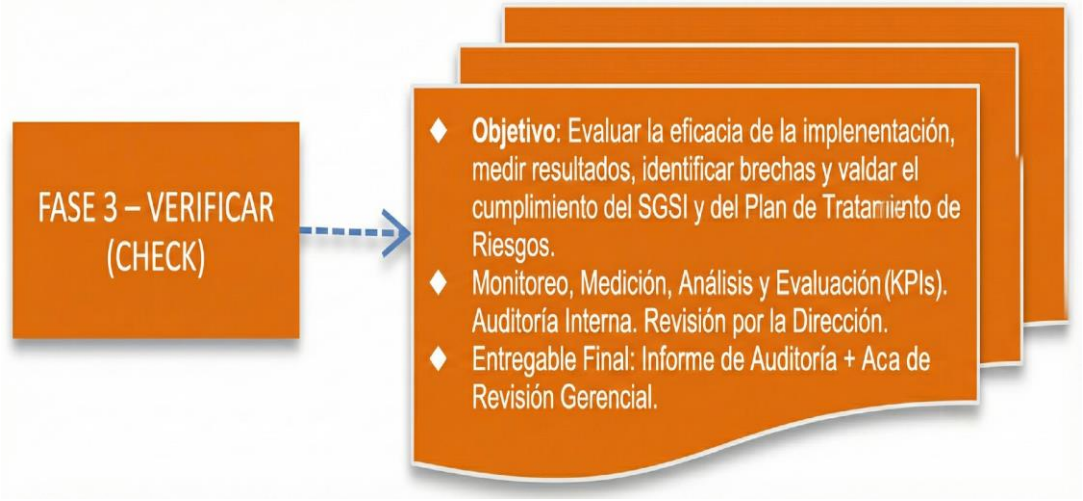



Figura 4: Fase de verificación del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

| Metas | Actividades / Instrumentos (ISO 27001:2022) | Resultados |
|---|---|---|
| Monitorear y medir la efectividad del Plan de Tratamiento de Riesgos de Seguridad y Privacidad | • Realizar seguimiento al estado de los controles implementados<br>• Evaluar la eficacia de los controles según riesgos residuales.<br>• Medir indicadores de seguridad definidos durante la planificación. | • Evidencias del desempeño y eficacia del plan.<br>• Identificación de brechas o desviaciones. |
| Verificar el cumplimiento de los procedimientos del SGSI y su aplicación | • Revisar registros, bitácoras, reportes y documentación generada durante la fase de implementación<br>• Validar cumplimiento de políticas, lineamientos y controles establecidos. | • Resultados documentados de cumplimiento.<br>• No conformidades o áreas de mejora identificadas. |
| Ejecutar auditoría interna al SGSI y al Plan de Tratamiento de Riesgos | • Realizar auditoría interna conforme.<br>• Evaluar conformidad con ISO/IEC 27001:2022 y con controles.<br>• Generar informe de hallazgos, no conformidades y observaciones. | • Informe de auditoría interna.<br>• Acciones correctivas necesarias identificadas. |
| Revisar y analizar los incidentes, vulnerabilidades y resultados de pruebas técnicas | • Validar registros de incidentes, vulnerabilidades, pruebas de intrusión y Ethical Hacking.<br>• Analizar tendencias, causas raíz y efectividad de la respuesta.<br>• Evaluar materialización de riesgos y controles asociados. | • Informe consolidado de riesgos nuevos o no mitigados.<br>• Actualización del nivel de riesgo residual. |

**FASE IV: ACTUAR**

Implementar acciones correctivas y de mejora continua para fortalecer el SGSI y optimizar el Plan de Tratamiento de Riesgos.

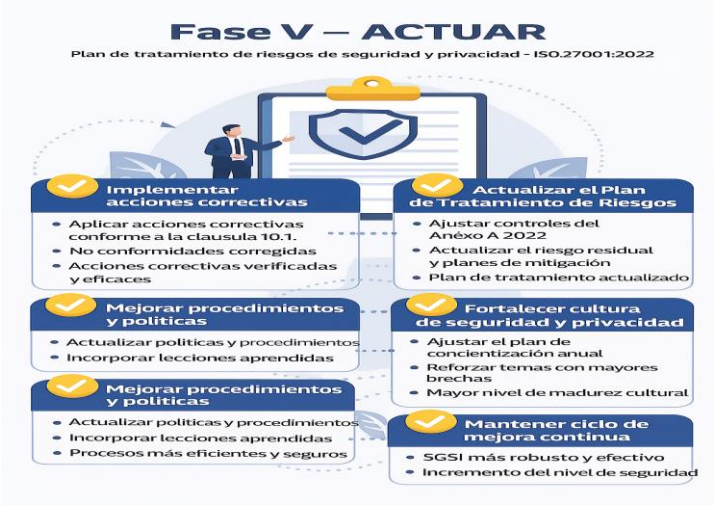



Figura 5: Fase de actuar del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

| Metas | Actividades / Instrumentos (ISO 27001:2022) | Resultados |
|---|---|---|
| Implementar acciones correctivas para tratar no conformidades identificadas | • Aplicar acciones correctivas.<br>• Registrar no conformidades, causas raíz y actividades de remediación.<br>• Verificar la eficacia de las acciones tomadas. | • No conformidades corregidas. • Evidencia de acciones correctivas y su efectividad. |
| Actualizar el Plan de Tratamiento de Riesgos según hallazgos y cambios en el contexto | • Revisar riesgos emergentes, incidentes, vulnerabilidades y brechas detectadas. según nuevas necesidades.<br>• Actualizar el riesgo residual y los planes de mitigación. | • Plan de tratamiento actualizado. • Controles fortalecidos o ajustados a riesgos reales. |
| Mejorar procedimientos, políticas y documentación del SGSI | • Actualizar políticas, procedimientos y lineamientos según resultados de auditorías<br>• Incorporar lecciones aprendidas y buenas prácticas. | • Documentación revisada y alineada con ISO 27001:2022. • Procesos más eficientes y seguros. |
| Fortalecer la cultura organizacional de seguridad y privacidad | • Ajustar el plan anual de concientización según debilidades encontradas. • Reforzar temas con mayores brechas: phishing, contraseñas, uso de información, etc. | • Mayor nivel de madurez cultural. • Reducción de comportamientos de riesgo. |
| Optimizar el desempeño del SGSI | • Refinar indicadores, métricas y métodos de medición (9.1). • Alinear mejoras con los objetivos estratégicos de la entidad. • Revisar recursos, roles y capacidades necesarias. | • SGSI más robusto y alineado a la estrategia institucional. • Aumento del nivel de madurez. |
| Mantener el ciclo de mejora continua del SGSI | • Repetir el ciclo PHVA con ajustes correspondientes. • Planificar nuevas mejoras y priorizar acciones estratégicas. | • Ciclo de mejora continua en ejecución permanente. • Incremento sostenido del nivel de seguridad y privacidad. |

## 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, las políticas nacionales de seguridad digital), estos roles incluyen:

**1.Alta Dirección**

- Supervisión Estratégica: responsable de garantizar que el Plan de Tratamiento de Riesgos esté alineado con los objetivos institucionales del Club Militar.
- Aprobación de Recursos: Asegura la disponibilidad de presupuesto y personal para la implementación de controles técnicos y administrativos.

**2.Grupo Gestión TIC (Líder de Seguridad y Privacidad)**

- Liderazgo Operativo: Actúa como el articulador de las fases de identificación, análisis y tratamiento de riesgos.
- Monitoreo Técnico: Ejecuta el monitoreo continuo de la infraestructura tecnológica, redes y sistemas para detectar vulnerabilidades.
- Gestión de Planes: Supervisa la ejecución del cronograma de actividades (como las pruebas de Ethical Hacking mencionadas en tu documento) y evalúa la eficacia de las medidas adoptadas.

**3. Jefes de Área y Coordinadores de Procesos**

- Dueños de Activos: Identifican los activos de información críticos en sus áreas (financiera, recreación, administrativa, etc.) y gestionan sus riesgos específicos
- Aseguramiento: Garantizan que los funcionarios y contratistas bajo su mando cumplan con las políticas de seguridad y los controles establecidos en el mapa de riesgos.

**4. Oficina de Control Interno**

- Evaluación Independiente: Realiza auditorías para verificar que el sistema de gestión de riesgos cumpla con la normativa ISO 27001 y los lineamientos de MinTIC.

- Validación de Controles: Evalúa si los controles implementados por el Grupo TIC y las áreas son suficientes para mitigar los riesgos identificados.

**5. Usuarios Finales (Servidores Públicos, Contratistas y Terceros)**

- Cultura de Seguridad: Son la primera línea de defensa. Deben cumplir con el manual de políticas y reportar cualquier incidente o sospecha de brecha de seguridad de manera inmediata.

## MARCO NORMATIVO Y CUMPLIMIENTO LEGAL EN EL CONTEXTO NACIONAL

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.

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

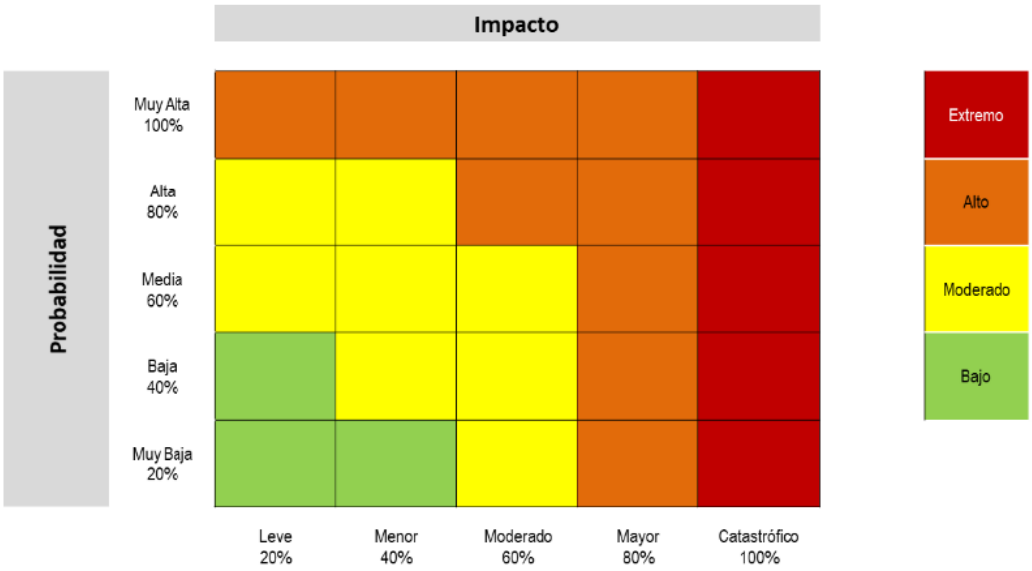
Tabla 2 Impacto del Riesgo

| **TABLA DE IMPACTO** | | |
|---|---|---|
| **NIVEL** | **DESCRIPTOR** | **DESCRIPCIÓN** |
| **1** | Leve | 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 3 Matriz de calificación, evaluación y respuesta a los riesgos.




*Fuente: Guía de Riesgos DAFP*

## 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 | 01-01-2026 | 31-06-2026 |
| 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 | 01-01-2026<br>01-04-2026<br>01-07-2026<br>01-10-2026 | 31-03-2026<br>31-06-2026<br>31-09-2026<br>31-12-2026 |
| 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 | 01-01-2026<br>01-04-2026<br>01-07-2026<br>01-10-2026 | 31-03-2026<br>31-06-2026<br>31-09-2026<br>31-12-2026 |

| | | | | | |
|---|---|---|---|---|---|
| **4** | Monitoreo y seguimiento de incidentes de seguridad | Informe de Riesgos | Grupo Gestión Tic | 01-01-2026<br>01-04-2026<br>01-07-2026<br>01-10-2026 | 31-03-2026<br>31-06-2026<br>31-09-2026<br>31-12-2026 |
| **5** | Auditorias y evaluaciones internas de seguridad | Informes de Auditoría Interna y Externa<br>Informe de Resultados de Evaluaciones de Riesgos | Oficina de Control Interno | 01-01-2026<br>01-07-2026 | 31-06-2026<br>31-12-2026 |
| **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 cómputo del Club Militar en sus 3 sedes | Grupo Gestión Tic | 01-01-2026<br>01-04-2026<br>01-07-2026<br>01-10-2026 | 31-03-2026<br>31-06-2026<br>31-09-2026<br>31-12-2026 |
| **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 | 01-10-2026 | 30-12-2026 |

## 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 Coordinadores 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

I. Referencia Institucional: Política de Seguridad y Privacidad de la Información
II. Referencia Institucional: Instructivo Gestión Incidentes Seguridad y Privacidad Información

III. Referencia Nacional Actualizada (MinTIC): Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - Versión 8 (Vigencia 2026).

IV. Guía Metodológica: Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) - Versión 5.0 (2025).

V. Marco Normativo de Riesgos: Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP

## 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 |
| **4** | 30-01-2026 | Se actualiza información acorde al SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI – MINTIC |

## VALIDACIÓN DE FIRMAS

| | NOMBRE | CARGO |
|---|---|---|
| **ELABORÓ:** | TASD. Javier Parra Pinzón | TASD. Grupo Gestión TIC |
| **REVISÓ:** | Yudyett Astrid Pulido Guevara | Sistemas Integrados de Gestión – OAP. |
| **APROBÓ:** | TASD. Javier Parra Pinzón | Coordinador Grupo Gestión TIC (E) |
| | PD. Elizabeth Hoyos Salazar | Jefe Oficina De Planeación. |
| | Dr. Edgardo Muñoz Chegwin | Jefe Oficina Asesora Jurídica. |
| **FIRMANTE:** | CR. Ernesto Santamaria Montenegro | Subdirector General del Club Militar. |

# REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL_03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20260130-183606-49b297-95282445

Estado: Finalizado

Creación: 2026-01-30 18:36:06

Finalización: 2026-01-30 19:32:49

Escanee el código para verificación

**Aprobación: ELIZABETH HOYOS SALAZAR**

Elizabeth Hoyos Salazar
39179008
ehoyos@clubmilitar.gov.co
Jefe de Oficina Asesora de Planeación
Club Militar

**Aprobación: Javier Parra Pinzon**

Javier Parra Pinzon
1012377884
jparra@clubmilitar.gov.co
Coordinador Grupo Gestión TICs (E)
Club Militar

**Revisión: Yudyett Astrid Pulido**

Yudyett Pulido
52915896
yapulido@clubmilitar.gov.co

**Elaboración: Javier Parra Pinzon**

Javier Parra Pinzon
1012377884
jparra@clubmilitar.gov.co
Coordinador Grupo Gestión TICs (E)
Club Militar

# REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL_03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20260130-183606-49b297-95282445

Estado: Finalizado

Creación: 2026-01-30 18:36:06

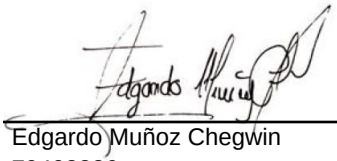
Finalización: 2026-01-30 19:32:49

Escanee el código para verificación

**Firma: Ernesto Santamaria Montenegro**

Ernesto Santamaria Montenegro
13617334
esantamaria@clubmilitar.gov.co
Subdirector General
Club Militar

**Aprobación: Edgardo Muñoz Chegwin**



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 2026

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20260130-183606-49b297-95282445

Creación: 2026-01-30 18:36:06

Estado: Finalizado

Finalización: 2026-01-30 19:32:49

Escanee el código para verificación

| TRAMITE | PARTICIPANTE | ESTADO | ENVIO, LECTURA Y RESPUESTA |
|---|---|---|---|
| Elaboración | Javier Parra Pinzon<br>jparra@clubmilitar.gov.co<br>Coordinador Grupo Gestión TICs (E)<br>Club Militar | Aprobado | Env.: 2026-01-30 18:36:08<br>Lec.: 2026-01-30 18:36:18<br>Res.: 2026-01-30 18:36:20<br>IP Res.: 168.90.12.20<br>Canal: Email |
| Revisión | Yudyett Pulido<br>yapulido@clubmilitar.gov.co | Aprobado | Env.: 2026-01-30 18:36:20<br>Lec.: 2026-01-30 18:39:49<br>Res.: 2026-01-30 18:39:54<br>IP Res.: 191.156.181.232<br>Canal: Email |
| Aprobación | Javier Parra Pinzon<br>jparra@clubmilitar.gov.co<br>Coordinador Grupo Gestión TICs (E)<br>Club Militar | Aprobado | Env.: 2026-01-30 18:39:55<br>Lec.: 2026-01-30 18:41:19<br>Res.: 2026-01-30 18:41:21<br>IP Res.: 168.90.12.20<br>Canal: Email |
| Aprobación | Elizabeth Hoyos Salazar<br>ehoyos@clubmilitar.gov.co<br>Jefe de Oficina Asesora de Planeación<br>Club Militar | Aprobado | Env.: 2026-01-30 18:41:21<br>Lec.: 2026-01-30 19:02:31<br>Res.: 2026-01-30 19:02:39<br>IP Res.: 191.156.155.134<br>Canal: Email |
| Aprobación | Edgardo Muñoz Chegwin<br>emunoz@clubmilitar.gov.co<br>Jefe Oficina Asesora Jurídica<br>CLUB MILITAR | Aprobado | Env.: 2026-01-30 19:02:39<br>Lec.: 2026-01-30 19:16:46<br>Res.: 2026-01-30 19:16:57<br>IP Res.: 186.102.117.190<br>Canal: Email |
| Firma | Ernesto Santamaria Montenegro<br>esantamaria@clubmilitar.gov.co<br>Subdirector General<br>Club Militar | Aprobado | Env.: 2026-01-30 19:16:58<br>Lec.: 2026-01-30 19:32:45<br>Res.: 2026-01-30 19:32:48<br>IP Res.: 168.90.12.20<br>Canal: Email |