PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2025

TABLA DE CONTENIDO

OBJETIVO

Establecer un marco de control y gestión que proteja los activos de información de la entidad, garantizando la confidencialidad, integridad y disponibilidad de dichos activos. Este plan tiene como fin prevenir, mitigar y gestionar los riesgos relacionados con la seguridad y privacidad de la información, asegurando el cumplimiento de las políticas de seguridad y normativas vigentes, promoviendo una cultura organizacional sólida en materia de seguridad y resguardando los datos sensibles frente a posibles amenazas tanto internas como externas.

OBJETIVO ESPECIFICOS:

- Evaluar y analizar los riesgos de seguridad digital relacionados con los activos de información para apoyar el cumplimiento de la misión de la entidad.
- Identificar amenazas e impactos de seguridad digital que puedan afectar los procesos y operaciones de la entidad, priorizando la protección de los activos de información.
- Definir e implementar controles de seguridad adecuados que respondan a los riesgos identificados y faciliten la toma de decisiones sobre el riesgo residual.
- Establecer un plan de tratamiento del riesgo residual que permita mitigar los riesgos y asegurar el cumplimiento de las políticas de seguridad digital de la entidad.
- Monitorear y ajustar continuamente los controles de seguridad para garantizar que se mantengan alineados con las necesidades y riesgos cambiantes de la entidad.

ALCANCE

El Plan de Seguridad y Privacidad de la Información se aplicará a todos los procesos, activos de información, sistemas y personal de la entidad, incluyendo a contratistas y terceros que manejen o accedan a información de la organización. Este plan abarca la implementación y el cumplimiento de políticas de seguridad de la información, siguiendo tanto la normativa vigente como las mejores prácticas de estándares internacionales, tales como el ISO 27001, para asegurar la confidencialidad, integridad, y disponibilidad de los datos y servicios digitales. La entidad adoptará un enfoque basado en el ciclo PHVA (Planear, Hacer, Verificar, Actuar) para garantizar la mejora continua y el control de los riesgos de seguridad y privacidad de la información, orientando sus acciones a mitigar, prevenir, transferir, o aceptar dichos riesgos de acuerdo con los niveles de tolerancia establecidos.

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

- **Ley 23 de 1982** – Sobre derechos de autor y derechos conexos.
- **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, y se establecen entidades de certificación.
- **Ley 962 de 2005** – Por la cual se dictan disposiciones sobre la racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejerzan funciones públicas o presten servicios públicos.
- **Ley 1032 de 2006** – Por medio de la cual se modifican algunos artículos del Código Penal en materia de delitos contra la propiedad intelectual y derechos de autor.
- **Ley 1266 de 2008** – Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- **Ley 1437 de 2011** – Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 1474 de 2011** – Por la cual se dictan normas orientadas al fortalecimiento de los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública (Estatuto Anticorrupción).
- **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.
- **Ley 1757 de 2015** – Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática.

2. Decretos

- **Decreto Ley 2150 de 1995** – Racionalización de trámites administrativos y simplificación normativa en la Administración Pública, con el fin de optimizar la eficiencia y accesibilidad de los servicios estatales
- **Decreto 527 de 1999** – Regulación del hábeas data, estableciendo disposiciones generales sobre el tratamiento de datos personales y la administración de bases de datos en Colombia.
- **Decreto 1747 de 2000** – Normativa para la infraestructura de certificación digital, regulando la creación y operación de entidades de certificación, así como la expedición y validez de certificados y firmas digitales.
- **Decreto 2364 de 2012** – Regulación del uso de la firma electrónica en Colombia, estableciendo su equivalencia funcional con la firma manuscrita y su aplicabilidad en documentos electrónicos, en concordancia con la Ley 527 de 1999 sobre comercio electrónico.
- **Decreto 2609 de 2012** – Reglamentación de la gestión documental en entidades públicas y privadas que cumplen funciones públicas, en cumplimiento de la Ley 594 de 2000 (Ley General de Archivos) y la Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo), estableciendo lineamientos para la organización, conservación y acceso a la información.
- **Decreto 1377 de 2013** – Reglamentación parcial de la Ley 1581 de 2012, estableciendo disposiciones específicas para la protección de datos personales, el tratamiento de información en bases de datos y las obligaciones de los responsables y encargados del tratamiento de datos en Colombia Decreto 2573 de 2014 - Crea la Ley de Transparencia y derecho de acceso a la información pública
- **Decreto 103 de 2015** – Reglamentación del acceso, uso y validez jurídica de los mensajes de datos, firmas digitales y firma electrónica, conforme a la Ley 527 de 1999, estableciendo lineamientos para su implementación en trámites y procesos administrativos.
- **Decreto 1078 de 2015** – Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (TIC), compilando y armonizando la normatividad existente en materia de telecomunicaciones, servicios postales y tecnologías digitales en Colombia.
- **Decreto 1494 de 2015** – Reglamentación parcial de la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública), estableciendo disposiciones sobre la publicación, divulgación y acceso a la información pública en entidades del Estado, garantizando el derecho fundamental a la información.
- **Decreto 1008 de 2018** – Definición de los lineamientos generales de la Política de Gobierno Digital, estableciendo directrices para la transformación digital del Estado, la interoperabilidad de los sistemas de información, la seguridad digital y la implementación de servicios ciudadanos digitales en Colombia

3. Resoluciones y Directivas

- **Resolución 00500 de marzo 10 de 2021** – Disposición normativa que establece lineamientos específicos en materia de [tema que regula la resolución], en el marco de la modernización y optimización de

procesos administrativos. (Si me indica el tema exacto de esta resolución, puedo afinar mejor su epígrafe).

- **Resolución 746 de 2022** – Adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) en Colombia, estableciendo lineamientos y directrices para la gestión de riesgos de seguridad digital, protección de la información y cumplimiento normativo en entidades públicas, en el marco de la Política de Gobierno Digital y la legislación en materia de seguridad de la información.
- **Directiva Presidencial 02** – Directrices para la implementación segura de la Política de Gobierno Digital, estableciendo los lineamientos para garantizar la seguridad, interoperabilidad y protección de los sistemas de información del Estado, asegurando la confianza y el acceso seguro a los servicios públicos digitales, en el marco de la transformación digital del sector público.
- **Políticas y Lineamientos**
- **CONPES 3701 de 2011** – Establece los lineamientos de política para la Ciberseguridad y Ciberdefensa en Colombia, orientados a la protección de infraestructuras críticas, la gestión de riesgos cibernéticos, y la promoción de una cultura de seguridad en el ciberespacio, con el fin de garantizar la defensa nacional frente a amenazas cibernéticas y asegurar la continuidad de los servicios esenciales del Estado
- **CONPES 3854 de 2016** – Establece las **directrices para la Política de Ciberseguridad y Ciberdefensa** en Colombia, con un enfoque en la protección de la infraestructura crítica del país, el fortalecimiento de capacidades nacionales en ciberseguridad, la colaboración internacional y la creación de marcos normativos y operacionales. para la prevención y respuesta ante ciberataques.
- **Políticas Técnicas de Seguridad de la Información de Función Pública (2020)** – Conjunto de directrices y procedimientos establecidos por la Función Pública para garantizar la seguridad de la información en el ámbito del sector público, incluyendo la protección de datos, la gestión de riesgos informáticos y el cumplimiento de normativas nacionales e internacionales sobre privacidad y seguridad de la información en el contexto gubernamental.

GLOSARIO

Para la adecuada gestión de riesgos de seguridad digital se debe manejar con propiedad los siguientes términos:

- **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)
- **Activo:** [Según ISO 27000]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Amenazas:** [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis del riesgo: [**NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Apetito de riesgo:** Es el nivel máximo de riesgo que la entidad está dispuesta a asumir.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000)

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Consecuencia:** [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.

- **Controles:** [Según ISO 27000]: 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. En una definición más simple, es una medida que modifica el riesgo.

- **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática

- **Criterios del riesgo:** [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

- **Evaluación del riesgo:** [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **Identificación del riesgo:** [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.

- **Impacto:** [Según ISO 27000]: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Inventario de activos:** [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

- **Nivel de riesgo:** [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.

- **Perfil del riesgo:** [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.

- **Política:** [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

- **Política:** para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

- **Reducción del riesgo:** [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

- **Riesgo:** [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo Residual:** [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.

- **Vulnerabilidad:** [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

  - ❖ SEVEN: Sistema ERP del Club Militar.
  - ❖ KACTUS: Sistema de Gestión del Talento Humano
  - ❖ AZ DIGITAL: Sistema de Gestión Documental del Club Militar.
  - ❖ SUITE VISIÓN: Sistema de Gestión Estratégica del Club Militar.
  - ❖ TIC ATENTO: Sistema de mesa de ayuda del Club Militar.

ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013 es de:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	80	100	GESTIONADO
A.9	CONTROL DE ACCESO	80	100	GESTIONADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	80	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	84	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	84	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	84	100	OPTIMIZADO
A.18	CUMPLIMIENTO	80	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**82**	**100**	OPTIMIZADO

CRONOGRAMA DE LAS ACTIVIDADES

No	Descripción	Evidencia	Responsable	Inicio de la Actividad	Término de la Actividad
1.	Sensibilización y socialización temas de seguridad y privacidad de la información, seguridad digital y continuidad del negocio al interior de la entidad.	Campañas de sensibilización de la política de seguridad de la información	Oficial de Seguridad de la Información Coordinación Grupo de 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
2.	Actualización de activos de información de la entidad.	Inventario de activos de información	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC	01-02-2025	30-12-2025
3.	Socializar en la entidad el documento para la identificación y clasificación de los activos de información y de activos para capacitar a los procesos con el fin de fortalecer el concepto de activo de información, sus tipos y cómo se clasifican.	Actas de reunión, capacitación o charla	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC Gestión Documental	01-05-2025	30-07-2025
4.	Capacitación a los funcionarios del Grupo de Gestión TIC en el Sistema de Gestión de Seguridad de la Información.	Actas de reunión, capacitación e inducción	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC	01-03-2025	31-03-2025
5.	Verificación de la cláusula de seguridad de la información de los contratos que los requieren.	Informe de la verificación a Clausulado del contrato	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC Coordinación Grupo de Gestión Administrativa	01-05-2025	30-06-2025
6.	Capacitar a los supervisores de contrato sobre la forma de asegurar y hacer seguimiento al cumplimiento de los requerimientos de seguridad de la información para los contratos que aplique.	Actas de reunión, capacitación e inducción	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC Coordinación Grupo de Gestión Administrativa	01-06-2025	30 de junio de 2025

7.	Ejecución análisis de vulnerabilidades.	Informe de vulnerabilidades	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC	01-10-2025	30-12-2025
8.	Generación, presentación y reporte de indicadores de seguridad y privacidad de la información.	Informe de monitoreo y evaluación de riesgos	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC	01-12-2025	30-12-2025
9	Sensibilización al personal sobre la Política de Tratamiento de Datos	Campañas de sensibilización sobre la Política de Tratamiento de Datos	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC Grupo Misional integral al socio	01-07-2025	30-09-2025

ROLES Y RESPONSABILIDADES

1. Alta Dirección

- Proporcionar apoyo y recursos para la implementación del plan.
- Demostrar un compromiso visible con la seguridad y privacidad de la información
- Revisar informes de auditoría y del CISO sobre el estado de la seguridad y privacidad de la organización

2. Oficina de Control Interno

- Realizar auditorías periódicas del cumplimiento de las políticas y controles de seguridad y privacidad de la información.
- Realizar evaluaciones objetivas para identificar áreas de mejora en la seguridad de la información, asegurando que las medidas de protección implementadas estén funcionando según lo previsto. .
- Supervisar que todas las Oficinas Asesoras, Grupos de Gestión y áreas de la entidad cumplan con las políticas, normas y procedimientos establecidos en el plan de seguridad y privacidad.
- Auditoría Interna Plan del Modelo de seguridad y privacidad de la información

- Llevar a cabo auditorías periódicas sobre los controles y políticas del MSPI, identificando y documentando hallazgos y brechas en la seguridad. Asegurar que se implementen las acciones correctivas necesarias.

3. Grupo de Gestión Talento Humano

- Realizar investigaciones de antecedentes a los candidatos asegura que las personas con acceso a información sensible cumplan con los estándares de confianza y seguridad de la organización. Con el fin de Mitigar el riesgo de acceso no autorizado a la información confidencial de la organización mediante la verificación del historial y la confiabilidad de los candidatos.

- Establecer claramente en los términos y condiciones del empleo las obligaciones de los empleados respecto a la seguridad y la privacidad de la información ayuda a consolidar un compromiso desde el inicio de la relación laboral.

- Garantizar que los empleados comprendan y acepten sus responsabilidades de seguridad y privacidad, incluyendo el manejo adecuado de la información y las consecuencias de no cumplir con estas políticas.

- Desarrollar y coordinar programas de capacitación periódica para todos los empleados sobre políticas de seguridad, privacidad y protección de datos.

- Asegurar que el personal esté constantemente informado sobre las mejores prácticas de seguridad, las políticas de la organización, y cómo reconocer y responder ante posibles amenazas de seguridad.

- Colaborar con el área de Control Interno y otras áreas relevantes para monitorear el cumplimiento de las políticas de seguridad y privacidad de los empleados. Esto incluye la participación en auditorías de seguridad.

- Implementar protocolos claros para cambios de rol, ascensos, transferencias, y, especialmente, desvinculaciones, asegurando que el acceso a los recursos de información se ajuste o elimine según corresponda.

- Dentro de la evaluación de desempeño Incluir criterios de seguridad y privacidad en la evaluación de desempeño del personal para incentivar el cumplimiento y promover la cultura de seguridad de la información.

4. Grupo de Gestión Administrativa

- Asegurarse de que todos los proveedores evaluados para el contrato cumplan con los requisitos mínimos de seguridad de la información.

- Incluir términos y condiciones en los contratos que definan claramente las obligaciones de los proveedores en cuanto a la seguridad de la información.

- Establecer un protocolo para gestionar cualquier incidente de seguridad que involucre a proveedores, coordinando con TIC para acciones técnicas correctivas.

- Verificar que los proveedores cuenten con certificaciones de seguridad (como ISO 27001) o políticas internas que aseguren la protección de la información.
- Incluir cláusulas contractuales que especifiquen los requisitos de seguridad de la información que el proveedor debe cumplir.
- Definir sanciones y acciones correctivas en caso de incumplimiento de las políticas de seguridad.
- Definir un proceso de desvinculación que asegure que el proveedor devuelve o destruye toda la información de la organización de manera segura al finalizar el contrato.

5. Grupo de Gestión TIC

5.1 Comité de seguridad de la información

- Asegurar que el plan esté alineado con los objetivos estratégicos de la organización.
- Revisar y aprobar políticas, procedimientos y normas relacionadas con la seguridad y privacidad de la información.
- Evaluar y priorizar los riesgos relacionados con la seguridad y privacidad de la información.
- Supervisar las auditorías internas y las revisiones del cumplimiento de los controles de seguridad.

6.Oficial de Seguridad de la Información (CISO)

- Desarrollar y mantener el Plan de Seguridad y Privacidad de la Información.
- Identificar, evaluar y gestionar los riesgos de seguridad de la información.
- Diseñar e implementar políticas y controles de seguridad y privacidad de la información.
- Coordinar las actividades de capacitación y concienciación en seguridad y privacidad de la información.
- Gestionar incidentes de seguridad, liderando el equipo de respuesta ante incidentes.
- Implementar y mantener las medidas de seguridad técnicas (firewalls, antivirus, cifrado, etc.).
- Realizar evaluaciones periódicas de vulnerabilidades y pruebas de penetración.
- Asegurar la disponibilidad de los sistemas y realizar copias de seguridad de datos.
- Gestionar y monitorear el acceso a los sistemas y la red, garantizando que los privilegios de acceso se otorguen y revisen adecuadamente.

7. Líderes de Proceso o Responsables de Áreas

- Identificar los activos de información que manejan y garantizar que sean protegidos.
- Asegurar que los procesos que manejan información cumplan con las políticas y controles de seguridad y privacidad de la organización.
- Colaborar en la identificación y gestión de riesgos relacionados con sus procesos específicos.
- Informar sobre posibles incidentes de seguridad de la información en sus áreas.

DOCUMENTOS DE REFERENCIA

- N/A

DOCUMENTOS DE APOYO

- POLITICA DE TRATAMIENTO Y PROTECCION DE DATOS PERSONALES

ANEXOS

- N/A

CONTROL DE CAMBIOS

VERSIÓN	FECHA DEL CAMBIO	DESCRIPCIÓN DE LA ACTUALIZACIÓN
1	01-08-2019	Creación de documento.
2	28/01/2021	Actualización de actividades
3	04/01/2023	Actualización de nombre, alineación al Modelo de Seguridad y Privacidad de la Información (MSPI) y Plan Estratégico Institucional
4	31-01-2024	Actualización vigencia 2024.
5	28-01-2025	Actualización vigencia 2025.

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) Juan Carlos Arenas Fonseca	Jefe Oficina De Planeación (E)
	Dr. Edgardo Muñoz Chegwin	Jefe Oficina Asesora Jurídica.
	TC (RA) (E) Juan Carlos Arenas Fonseca	Subdirector General del Club Militar (E)
FIRMANTE:	BG (RA) José Henry Pinto Rodríguez	Director General del Club Militar.

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL-05 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2025.

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20250130-155734-a08336-10866498

Creación: 2025-01-30 15:57:34

Estado: Finalizado

Finalización: 2025-01-31 07:57:31

Escanee el código para verificación

Aprobación: Jefe Oficina De Planeación (E)

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-05 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2025.

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20250130-155734-a08336-10866498

Estado: Finalizado

Creación: 2025-01-30 15:57:34

Finalización: 2025-01-31 07:57:31

Escanee el código para verificación

Firma: Director General del Club Militar.

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

Aprobación: Subdirector General del Club Militar (E)

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-05 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2025.

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20250130-155734-a08336-10866498

Creación: 2025-01-30 15:57:34

Estado: Finalizado

Finalización: 2025-01-31 07:57:31

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 15:57:35 Lec.: 2025-01-30 15:58:40 Res.: 2025-01-30 15:59:08 IP Res.: 191.156.181.96
Revisión	Yudyett Pulido yapulido@clubmilitar.gov.co	Aprobado	Env.: 2025-01-30 15:59:08 Lec.: 2025-01-30 15:59:21 Res.: 2025-01-30 15:59:36 IP Res.: 200.91.222.50
Aprobación	Javier Parra Pinzon jparra@clubmilitar.gov.co ASSD Club Militar	Aprobado	Env.: 2025-01-30 15:59:36 Lec.: 2025-01-30 15:59:50 Res.: 2025-01-30 16:00:01 IP Res.: 186.31.211.184
Aprobación	JUAN CARLOS ARENAS jcarenas@clubmilitar.gov.co	Aprobado	Env.: 2025-01-30 16:00:01 Lec.: 2025-01-30 18:06:57 Res.: 2025-01-30 18:07:07 IP Res.: 191.95.52.76
Aprobación	Edgardo Muñoz Chegwin emunoz@clubmilitar.gov.co Jefe Oficina Asesora Jurídica CLUB MILITAR	Aprobado	Env.: 2025-01-30 18:07:07 Lec.: 2025-01-30 18:07:22 Res.: 2025-01-30 18:51:06 IP Res.: 152.203.150.157
Aprobación	JUAN CARLOS ARENAS jcarenas@clubmilitar.gov.co	Aprobado	Env.: 2025-01-30 18:51:07 Lec.: 2025-01-30 18:51:36 Res.: 2025-01-30 18:51:44 IP Res.: 181.68.166.41
Firma	Brigadier General (RA) José Henry Pin asistentedireccion@clubmilitar.gov.co Director General Club Militar	Aprobado	Env.: 2025-01-30 18:51:44 Lec.: 2025-01-30 19:14:56 Res.: 2025-01-31 07:57:31 IP Res.: 190.109.17.26