PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DEL CLUB MILITAR 2026

TABLA DE CONTENIDO

OBJETIVO

Establecer y mantener un marco de Gobernanza de Seguridad Digital y Privacidad de la Información en el Club Militar, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma NTC-ISO/IEC 27001. Este plan busca garantizar la confidencialidad, integridad y disponibilidad de los activos de información estratégicos y misionales, gestionando los riesgos de seguridad digital y asegurando la continuidad de la operación frente a incidentes cibernéticos.

OBJETIVO ESPECIFICOS:

- **Fortalecer la Gobernanza**: Implementar las instancias y roles definidos en el Decreto 338 de 2022, asegurando la toma de decisiones estratégicas frente a riesgos digitales.
- **Gestión de Riesgos:** Identificar, analizar y tratar los riesgos de seguridad digital y privacidad que afecten los procesos misionales y de apoyo del Club Militar, aplicando la metodología definida por la Función Pública. 3.
- **Cumplimiento Normativo:** Garantizar la adopción de los lineamientos de la Resolución 500 de 2021 y Resolución 746 de 2022, cerrando la brecha de cumplimiento frente a los controles del Anexo A de la norma ISO/IEC 27001 (Versión 2022).
- **Protección de Datos:** Asegurar el cumplimiento de la Ley 1581 de 2012 mediante la actualización periódica del Registro Nacional de Bases de Datos (RNBD) y la protección de datos sensibles de los socios y funcionarios.
- **Cultura de Seguridad**: Ejecutar el plan de sensibilización y capacitación para fomentar hábitos seguros en el uso de los recursos tecnológicos del Club.

ALCANCE

El Plan de tratamiento de riesgos de seguridad digital y privacidad de la información, incluido su tratamiento será aplicado a todos procesos y activos de información del Club Militar. La metodología definida por la entidad para la gestión del riesgo es la de Función Pública, complementado con buenas prácticas con el ISO-27005, con el fin mitigar, retener, transferir o asumir los riesgos.

NORMATIVIDAD

Leyes

- Resolución 02277 de 2025 (MinTIC): "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se establecen los nuevos lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI)".
- Resolución 00860 de 2025 (MinTIC): "Por la cual se establece el Modelo Integrado de Gestión (MIG) y la articulación con el Sistema de Gestión de Seguridad de la Información (SGSI)".

- Ley 2294 de 2023 (Plan Nacional de Desarrollo): "Marco para la transformación digital y seguridad digital en entidades públicas 2022-2026".

Decretos

- Decreto 1078 de 2015 (Título 21 - Adicionado por Decreto 338 de 2022): Establece los lineamientos generales para fortalecer la Gobernanza de la Seguridad Digital en las entidades del Estado.
- Decreto 767 de 2022: Establece los lineamientos generales de la Política de Gobierno Digital.
- Decreto 620 de 2020: Lineamientos generales en el uso y operación de los servicios ciudadanos digitales (Autenticación Digital, Carpeta Ciudadana).
- Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012.

Resoluciones y Estándares

- Resolución 500 de 2021 (MinTIC): Adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital.
- Resolución 746 de 2022 (MinTIC): Fortalece el MSPI y define lineamientos adicionales de ciberseguridad.
- NTC-ISO/IEC 27001:2022: Norma Técnica Colombiana para Sistemas de Gestión de Seguridad de la Información (Versión actualizada).
- Resolución 1519 de 2020 (MinTIC): Estándares de publicación de información y seguridad digital.

Documentos de Política (CONPES)

- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.

GLOSARIO

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

- 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.
- Amenaza: [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.
- 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.
- Seguridad Digital: Situación de normalidad que el Club Militar busca preservar en el uso del entorno digital, gestionando los riesgos para generar confianza en sus procesos (Fuente: Decreto 1078/2015).
- CISO (Chief Information Security Officer): Rol estratégico del Oficial de Seguridad de la Información, encargado de articular la seguridad digital con los objetivos misionales del Club.

CRONOGRAMA DE LAS ACTIVIDADES

N°	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	01-01-2026 01-04-2026 01-07-2026 01-10-2026	30-03-2026 30-06-2026 30-09-2026 31-12-2026
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	01-02-2026	30-12-2026
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	01-04-2026	30-08-2026
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	01-02-2026	30-11-2026
5.	Verificación de la cláusula de seguridad de la información de los contratos que los requieren.	Clausulado del contrato	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC Coordinación Grupo de Gestión Administrativa	01-02-2026	30-06-2026
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	01-03-2026	30-07-2026

7.	Ejecución análisis de vulnerabilidades.	Informe de vulnerabilidades	Oficial de Seguridad de la Información Coordinación Grupo de Gestión TIC	01-10-2026	30-12-2026
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	01-12-2026	30-12-2026
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	01-07-2026	15-12-2026

DOCUMENTOS DE REFERENCIA

- NTC-ISO/IEC 27001:2022 – Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.
- NTC-ISO 31000:2018 – Gestión del riesgo. Directrices.
- Resolución 500 de 2021 (MinTIC) – 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.
- Resolución 746 de 2022 (MinTIC) – Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales.
- Resolución 1519 de 2020 (MinTIC) – Estándares y directrices para publicar información y requisitos de seguridad digital.
- CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital.
- Guía de Gestión de Riesgos de Seguridad de la Información – Departamento Administrativo de la Función Pública (DAFP) y MinTIC.
- Manual de Gobierno Digital – Ministerio de Tecnologías de la Información y las Comunicaciones (Versión vigente).

DOCUMENTOS DE APOYO

- Política de Seguridad y Privacidad de la Información

ANEXOS

- N/A

CONTROL DE CAMBIOS

VERSIÓN	FECHA DEL CAMBIO	DESCRIPCIÓN DE LA ACTUALIZACIÓN
4	31-01-2023	Actualización vigencia 2024.
5	28-11-2025	Actualización vigencia 2025.
6	30-01-2026	Actualización vigencia 2026

VALIDACIÓN DE FIRMAS

	NOMBRE	CARGO
ELABORO:	TASD. Javier Parra Pinzón	TASD Grupo Gestión Tics
REVISO:	TASD. Yudyett Astrid Pulido Guevara	Sistemas Integrados de Gestión – OAP.
APROBO:	TASD Javier Parra Pinzón	Coordinador Grupo Gestión Tics (E)
	PD. Elizabeth Hoyos Salazar	Jefe Oficina Asesora de Planeación
	Edgardo Muñoz Chegwin	Jefe Oficina Asesora Jurídica
FIRMANTE:	Coronel Ernesto Santamaria Montenegro	Subdirector General del Club Militar.

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL-05 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2026.

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20260130-143250-b42549-80543974

Creación: 2026-01-30 14:32:50

Estado: Finalizado

Finalización: 2026-01-30 17:12:31

Escanee el código para verificación

Aprobación: PD. Elizabeth Hoyos Salazar Jefe Oficina Asesora de Planeación

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

Aprobación: TASD Javier Parra Pinzón Coordinador Grupo Gestión Tics (E)

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

Revisión: TASD. Yudyett Astrid Pulido Guevara Sistemas Integrados de Gestión ? OAP.

Yudyett Pulido
52915896
yapulido@clubmilitar.gov.co

Elaboración: TASD. Javier Parra Pinzón TASD Grupo Gestión Tics

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

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL-05 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2026.

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20260130-143250-b42549-80543974

Estado: Finalizado

Creación: 2026-01-30 14:32:50

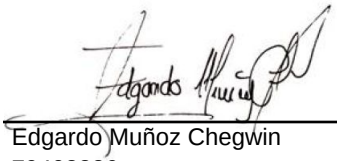
Finalización: 2026-01-30 17:12:31

Escanee el código para verificación

Firma: Coronel Ernesto Santamaria Montenegro Subdirector General

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

Aprobación: Edgardo Muñoz Chegwin 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 2026.

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20260130-143250-b42549-80543974

Creación: 2026-01-30 14:32:50

Estado: Finalizado

Finalización: 2026-01-30 17:12:31

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Javier Parra Pinzon jparra@clubmilitar.gov.co Coordinador Grupo Gestión TICs (E) Club Militar	Aprobado	Env.: 2026-01-30 14:32:53 Lec.: 2026-01-30 14:34:55 Res.: 2026-01-30 14:35:03 IP Res.: 168.90.12.20 Canal: Email
Revisión	Yudyett Pulido yapulido@clubmilitar.gov.co	Aprobado	Env.: 2026-01-30 14:35:03 Lec.: 2026-01-30 14:42:37 Res.: 2026-01-30 14:42:42 IP Res.: 168.90.12.20 Canal: Email
Aprobación	Javier Parra Pinzon jparra@clubmilitar.gov.co Coordinador Grupo Gestión TICs (E) Club Militar	Aprobado	Env.: 2026-01-30 14:42:42 Lec.: 2026-01-30 15:11:25 Res.: 2026-01-30 15:11:28 IP Res.: 168.90.12.20 Canal: Email
Aprobación	Elizabeth Hoyos Salazar ehoyos@clubmilitar.gov.co Jefe de Oficina Asesora de Planeación Club Militar	Aprobado	Env.: 2026-01-30 15:11:28 Lec.: 2026-01-30 15:13:26 Res.: 2026-01-30 15:13:34 IP Res.: 38.211.144.148 Canal: Email
Aprobación	Edgardo Muñoz Chegwin emunoz@clubmilitar.gov.co Jefe Oficina Asesora Jurídica CLUB MILITAR	Aprobado	Env.: 2026-01-30 15:13:34 Lec.: 2026-01-30 16:40:59 Res.: 2026-01-30 16:41:31 IP Res.: 38.211.144.148 Canal: Email
Firma	Ernesto Santamaria Montenegro esantamaria@clubmilitar.gov.co Subdirector General Club Militar	Aprobado	Env.: 2026-01-30 16:41:31 Lec.: 2026-01-30 17:12:16 Res.: 2026-01-30 17:12:31 IP Res.: 168.90.12.20 Canal: Email