PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR

2022

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El Club Militar hace parte de las entidades públicas que ha apropiado las iniciativas del Gobierno Nacional y las ha desplegado en todos sus niveles organizacionales, incluyéndolas en los objetivos estratégicos de la entidad.

La información para el Club Militar es considerada uno de los activos más importantes y de vital importancia para la toma de decisiones al interior de la entidad, generando mejor servicio e innovación a sus Socios.

Club Militar para cumplir y asegurar el direccionamiento estratégico, establece la compatibilidad de la política y de los objetivos de seguridad de la información que corresponden a:

- Fortalecer el sistema de gestión de seguridad de la información.
- Garantizar la continuidad del negocio - BCP
- Proteger los activos de información.
- Mitigar los riesgos del Club Militar.
- Apoyar la innovación tecnológica.
- Revisar y actualizar las políticas, procedimientos de seguridad de la información.

2 OBJETIVO GENERAL

Generar buenas prácticas de seguridad y privacidad de la información alineado al MSPI, con el fin de fortalecer los servicios de TI y asegurar la confidencialidad, integridad y disponibilidad de la información al interior del Club Militar.

3 Objetivos específicos

- Revisar y actualizar los riesgos de seguridad y privacidad de la información dentro el SGC para identificar cuales puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Cumplimiento a la estrategia de Gobierno Digital y Transformación Digital.
- Realizar campañas de conocimiento y sensibilización en seguridad y privacidad de la información del Club Militar

4 ALCANCE

El plan de seguridad y privacidad de la información es transversal y aplica a todos los procesos del Club Militar, en donde se desarrolle recolección, procesamiento, recuperación, almacenamiento y consulta de información, al cumplimiento de la misión y objetivos estratégicos del Club Militar.

5 DEFINICIONES Y SIGLAS

5.1 Definiciones

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

- **Confidencialidad:** Propiedad de la información, por la que se garantiza que esta accesible únicamente a personal autorizado a acceder a dicha información.
- **Integridad:** Se refiere a la correctitud y completitud de la información en una base de datos.
- **Administración del riesgo:** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que pueden afectar a la información.
  Dicho proceso es cíclico y debe llevarse a cabo de forma periódica.
- **Disponibilidad:** Garantizar que la información crítica y la capacidad de procesamiento puedan ser resguardadas y recuperadas rápida y completamente en caso de que ocurra alguna contingencia que interrumpa la continuación de las operaciones.

- **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.

- **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.

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

- **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.

6 ROLES Y RESPONSABILIDADES

Es responsabilidad del Comité de Seguridad de la Información del Club Militar, la implementación, aplicación, seguimiento, seguimiento y autorizaciones de la Política del Plan de Seguridad y Privacidad de la Información en las diferentes áreas y procesos del Club Militar, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión.

7 CUMPLIMIENTO

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios del Club Militar o terceros violan este Plan y los acuerdos de confidencialidad, el Club Militar se reserva el derecho de tomar medidas correspondientes.

8 COMUNICACIÓN

Mediante socialización a todos los funcionarios del Club Militar con sus diferentes medios de comunicación se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, igualmente estarán publicados en la página de la entidad www.clubmilitar.gov.co.

9 MONITOREO

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

10 DESCRIPCIÓN DE LAS POLÍTICAS

10.1 Generalidades

El Club Militar en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad.

11 DERECHOS MORALES Y PATRIMONIALES

Los usuarios son responsables de la custodia y la confidencialidad de los datos y la información a la cual tengan acceso en forma directa e indirecta.

El Club Militar es propietario de todos los datos e información que circule o se genere al interior de la misma o que esté disponible a través de sus sistemas de información y/o computadores.

12 DIVULGACION DE LA INFORMACION

La información entregada a los medios de comunicación debe hacerse a través del funcionario encargado del manejo de las comunicaciones del Club Militar.

Club Militar no se hace responsable por las consecuencias que se deriven de la utilización inadecuada por parte de terceros. Igualmente, se abstiene de suministrar la información que haya recibido de terceros para su uso interno y confidencial.

13 INFORMACIÓN CONFIDENCIAL

Exigir a los usuarios la protección de la información clasificada como confidencial o de uso restringido. Incluir una cláusula de confidencialidad en los contratos u órdenes, cuando el contratista requiera acceder de manera directa o indirecta a los datos o información de la entidad.

Todo empleado tenga acceso a la información, debe guardar confidencialidad sobre la misma. Todos los usuarios que necesiten acceso a cualquier recurso informático o sistema de información debe diligenciar el acuerdo de confidencialidad de la información **GT-M01-F01 COMPROMISO DE CONFIDENCIALIDAD.**

14 RECURSOS INFORMÁTICOS

Establecer el cambio periódico de los recursos informáticos, dependiendo de la obsolescencia, la vida útil, el estado de los mismos y las necesidades del Club Militar.

Se dará de baja a los equipos teniendo en cuenta el procedimiento establecido para tal fin.

Exigir a los usuarios la utilización responsable y razonable de los recursos informáticos. Igualmente, el acatamiento de las medidas de control establecidas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde con la importancia de los datos y la naturaleza de los riesgos.

15 DERECHOS DE AUTOR LICENCIAS DE SOFTWARE

- Proteger el Derecho de Autor y Derechos Conexos, de acuerdo con lo consagrado en la constitución política, los ordenamientos legales y acuerdos regionales.
- Mantener los sistemas de información y programas en las últimas versiones del software disponible en el mercado, para disminuir los problemas ocasionados por la diferencia de versiones.
- Todos los programas utilizados en los computadores del Club Militar deben contar con sus respectivas licencias de uso vigentes y condiciones exigidas.

16 CORREO ELECTRONICO

El Club Militar suministrara el acceso al correo electrónico y a internet, como herramientas para la realización de las labores, dependiendo de las responsabilidades y naturaleza del trabajo contratado, conforme a lo previsto en el manual de funciones.

El uso inadecuado de internet constituirá una falta grave, que se clasificará como tal por la magnitud del hecho o por no atender los requerimientos del Club Militar para que se cese la utilización indebida. La comprobación y las sanciones disciplinarias se realizarán conforme lo establecido en la legislación aplicable.

17 COMPUTADORES, SERVIDORES Y REDES

Prohibir a los usuarios la modificación de la configuración de hardware y software establecida por el funcionario encargado de administrar el sistema.

Club Militar garantizara que los equipos se protejan para disminuir el riesgo de hurto, destrucción, fluctuaciones de energía, incendio y medio ambiente (por ejemplo: agua), utilizando instalaciones en condiciones adecuadas, cerraduras, vigilantes, protectores contra transitorios de energía eléctrica y, para los servidores, fuentes de poder interrumpibles (UPS).

Prohibir el uso de módems en computadores que tengan conexión a la red local (LAN), para prevenir la intrusión de hackers a través de las puertas traseras. Todas las comunicaciones de datos deben efectuarse a través de la red LAN de la entidad.

18 CUENTAS DE LOS USUARIOS

Exigir que la solicitud de una nueva cuenta o el cambio de privilegios tenga las autorizaciones necesarias para su cambio, al mismo tiempo se debe diligenciar el **GT-M01-F04 FORMULARIO SOLICITUD ACCESO SERVICIOS INFORMATICOS** para el control de cambios y permisos que se requieran.

Cuando el Club Militar vincula a un funcionario este debe firmar un documento donde declara conocer las políticas informáticas y de seguridad de la información y acepta las responsabilidades.

No debe concederse una cuenta a personas que no sean empleados del Club Militar.

19 IDENTIFICACION, CONTRASEÑAS Y AUTORIZACIONES

Todos los usuarios que acceden a los sistemas de información requieren de un único e intransferible identificador, el cual será proporcionado como parte del proceso de autorización.

Los identificadores concedidos deberán eliminarse o deshabilitarse, cuando cese la vinculación del usuario con el Club Militar en forma permanente o temporal, o cuando se presente un uso indebido.

De esta manera, todas las acciones realizadas con un identificador de usuario son responsabilidad del titular.

El Grupo de Gestión Talento Humano debe informar cada vez que se retira un funcionario por terminación de contrato o por salida a vacaciones para que el Grupo de Gestión de TIC bloquee el usuario y así mitigar el riesgo en la Seguridad y Privacidad de la Información.

Para el personal que trabaja para el Club militar con un contrato de prestación de servicios el Grupo de Gestión Administrativa debe informar cuando finalice un contrato al Grupo de Gestión de TIC para que se bloquee el usuario.

20 ACTIVIDADES

1. Revisión de la Política de Seguridad y Privacidad de la Información.
2. Reunión con el Comité de Seguridad y Privacidad de la Información
3. Implementación de las Políticas de la Seguridad de la Información.

3.1. Entrevista y socialización con los líderes de los Procesos y Coordinadores.

4. Aprobación y adopción de las políticas de seguridad y privacidad de la información.
6. Aspectos de seguridad y privacidad de la información en la gestión de continuidad del negocio.
5. Seguimiento y Control de las políticas.

CRONOGRAMA DE ACTIVIDADES PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR												
ACTIVIDAD	2022											
	1 CUATRIMESTRE				2 CUATRIMESTRE				3 CUATRIMESTRE			
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Revisión de las Políticas de Seguridad y Privacidad de la Información												
Reunión del Comité de Seguridad de la Información												
Implementación de las Policitas de Seguridad y Privacidad de la Información												
Entrevista y Socialización con los líderes del Procesos y Coordinadores												
Aspectos de seguridad y privacidad de la información en la gestión de continuidad del negocio.												
Seguimiento y Control												

Este documento está alineado con:

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL DEL CLUB MILITAR

PLAN ESTRATEGICO PETIC 2022

RESOLUCIÓN 702 COMITE DE SEGURIDAD DE LA INFORMACION

CATÁLAGO DE SERVICIOS CLUB MILITAR

21. Control de cambios

Versión	Fecha del cambio	Descripción de la modificación
1	08/01/2019	Creación del documento
2	28/01/2021	Actualización de actividades
3	29/01/2022	Actualización de cronograma

ELABORÓ	REVISÓ	APROBÓ
Firma Nombre: Ing. ROSA ANGELINA MONCADA CASTILLO Cargo: Coordinadora Grupo de Gestión TIC	Firma Nombre: CN. (RA) CHRISTIAN HENRIQUE GONZÁLEZ RODRIGUEZ Cargo: Jefe oficina Asesora de Planeación	Firma Nombre: Vicealmirante (RA) HECTOR ALFONSO MEDINA TORRES Cargo: Director General