PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2024

TABLA DE CONTENIDO

OBJETIVO

Establecer para el Club Militar una guía que proporcione una metodología adecuada para el tratamiento de los riesgos y que esta permita identificar los roles de cada una de las partes y los responsables de cada activo de información que gestionarán dichos riesgos orientados a seguridad y privacidad de la información con el fin de minimizar la probabilidad que se materialice una amenaza y un posible alto impacto en la Entidad.

OBJETIVO ESPECIFICOS:

- Evaluar y analizar los riesgos de seguridad digital relacionados a los activos de información para facilitar el desarrollo de la misionalidad del Club Militar.
- Identificar las amenazas e impactos de seguridad digital asociadas a los procesos de la entidad.
- Identificar e implementar controles que atiendan la gestión de riesgos y facilite la toma de decisiones sobre el riesgo residual.
- Definir el plan de tratamiento del riesgo residual de la entidad.

ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información está orientado para ser aplicado a toda la entidad, sus servidores públicos, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios de tecnología de la información del Club Militar.

REFERENCIA

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

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la 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, Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
- Ley estatutaria 1581 de 2012, Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
- Ley 1474 de 2011, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
- 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 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- 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.
- CONPES 3854 de 2016, Política Nacional de Seguridad Digital.
- Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- 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 1494 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones

Requisitos técnicos

- 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.

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.

PROFUNDIZACION DEL PLAN

Ciclo de operación

El Plan de tratamiento de riesgos de seguridad y privacidad de la información se estableció teniendo en cuenta las cinco (5) fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información como habilitador de la política de Gobierno Digital del Gobierno Nacional (Ministerio de Tecnologías de la Información y las Comunicaciones, n.d.)

Figura 1: Ciclo del Modelo de Seguridad y Privacidad de la Información (Ministerio de Tecnologías de la Información y las Comunicaciones, n.d.)

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

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

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

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

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

Alineación del ciclo de operación con la norma ISO 27001:2013

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos de seguridad y privacidad de la información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) de la siguiente forma:

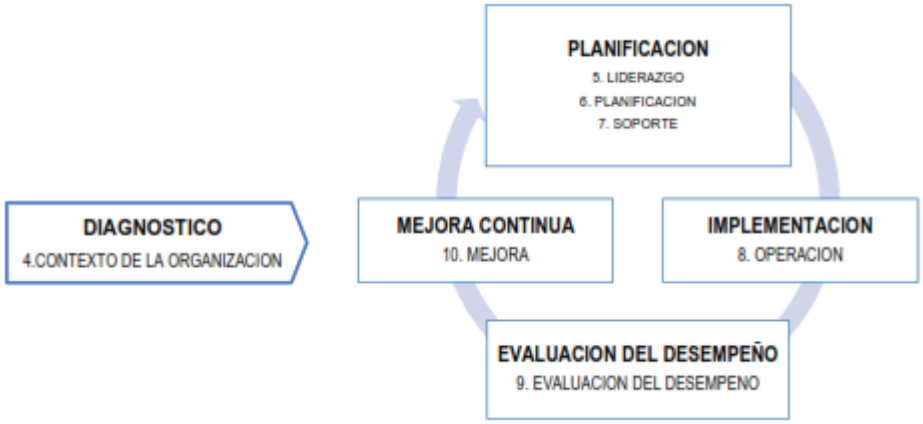

Figura 1: Norma ISO 27001:2013 alineado al Ciclo de mejora continua

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

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

- Fase diagnostico en la norma ISO 27001:2013: En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del modelo de seguridad de la información.
- Fase planeación en la norma ISO 27001:2013: En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos respecto a la seguridad y privacidad de la Información y entre otros

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

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

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

Fase I: Diagnostico

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

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

Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la seguridad y privacidad de la información al interior de la entidad.	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información. Diagnostico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013. Valoración estado actual de la seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.

Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad.	Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

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

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

Fase II: Planificación

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

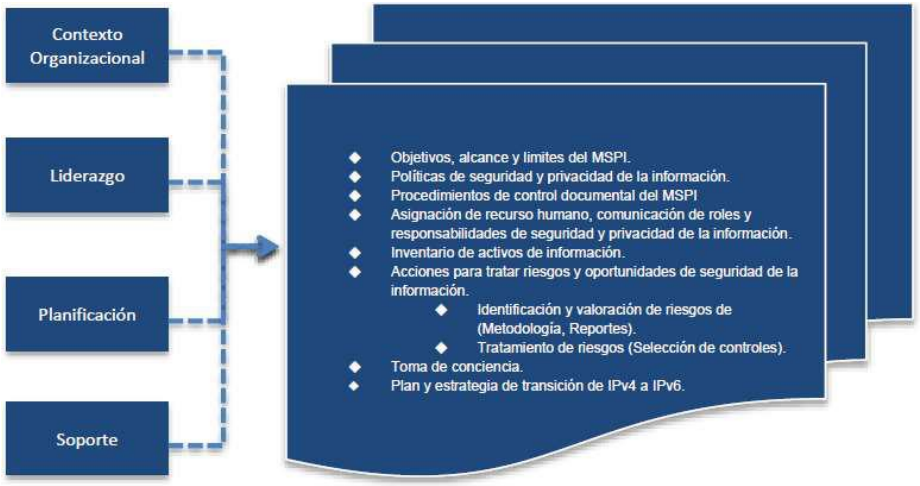

Figura 3: Fase de planificación del plan de tratamiento de riesgos de seguridad y privacidad de la información.

Metas	Actividades \ Instrumentos \ Resultados
Realizar un análisis de Contexto y factores externos e internos de la entidad en torno a la seguridad de la información.	Realizar un análisis de contexto de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. Contexto de la

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

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

Fase III: Implementación

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

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

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

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

Fase IV: Evaluación de desempeño

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

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

Metas	Actividades \ Instrumentos \ Resultados
Ejecución de auditorías de seguridad y privacidad de la información.	Ejecución de auditorías del Plan de tratamiento de riesgos de seguridad y privacidad de la información y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado. Las auditorías internas se deberán llevar a cabo para la revisión del

	Plan de tratamiento de riesgos de seguridad y privacidad de la información implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos cumplan con los requisitos establecidos en la norma ISO 27002:2013.
Plan de seguimiento, evaluación y análisis de Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Elaboración documento con el plan de seguimiento, evaluación y análisis del Plan de tratamiento de riesgos de seguridad y privacidad de la información revisado y aprobado.

Fase V: Mejora continua

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

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

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

MONITOREO, SEGUIMIENTO Y EVALUACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración interactiva de los riesgos de seguridad y privacidad de la información. Los riesgos son dinámicos como la misma entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos.
- Nuevas amenazas.
- Cambios o aparición de nuevas vulnerabilidades.

- Aumento de las consecuencias o impactos.
- Incidentes de seguridad de la información.

El monitoreo Trimestral o en el momento que se determine, debe estar a cargo de los responsables de los procesos, el jefe de la oficina asesora de planeación, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.

Tabla 1Probabilidad de riesgo

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

Tabla 2 Impacto del Riesgo

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

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

Riesgo inherente: Criticidad=probabilidad*Impacto

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

PROBABILIDAD	**IMPACTO**				
	Catastrófico	**Mayor**	**Moderado**	**Menor**	**insignificante**
Casi Seguro	**25**	**20**	**15**	**10**	**5**
Probable	**20**	**16**	**12**	**8**	**4**
Posible	**15**	**12**	**9**	**6**	**3**
Improbable	**10**	**8**	**6**	**4**	**2**
Raro	**5**	**4**	**3**	**2**	**1**

Fuente: Guía de Riesgos DAFP

Criticidad	**Extremo**	**Alto**	**Moderado**	**Bajo**
Rango	**25,20,16,15**	**12,10,9**	**8,6,5**	**4,3,2,1**

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 de documentación técnica como; NTC-ISO/IEC27002:2015, NTC-ISO/IEC 27001:2013, de 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.
- 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.	**Revisar y verificar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación identificados.** ● **Descripción de la actividad:** Se debe revisar, actualizar y verificar la Política y metodología de gestión de riesgos del Club Militar.	*Informes de Auditoría Interna y Externa *Informe de Resultados de Evaluaciones de Riesgos *Informe de Registros de Incidentes Previos *Informe de Revisiones de Políticas y	Grupo Gestión Tic	01 de marzo 2024	30 de diciembre 2024

		Procedimientos *Informe de Registro de Mejoras Implementadas. *Informe de Documentación de Capacitación y Concientización. *Informe de Resultados de Simulacros de Continuidad Operativa. Informe de Registros de Revisiones Periódicas			
	Sensibilizar y socializar temas de seguridad y privacidad de la información, seguridad digital y continuidad del negocio al interior de la entidad ● Se debe llevar a cabo reuniones sobre campañas de seguridad y privacidad de la información.	Son las 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 de Febrero 2024	30 de Diciembre 2024

DOCUMENTOS DE APOYO

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2. INSTRUCTIVO GESTION INCIDENTES SEGURIDAD Y PRIVACIDAD INFORMACION

ANEXOS

- N/A

CONTROL DE CAMBIOS

VERSIÓN	FECHA DEL CAMBIO	DESCRIPCIÓN DE LA ACTUALIZACIÓN
1	10-08-2023	Creación de documento.
2	31-01-2024	Actualización de actividades vigencia 2024.

VALIDACIÓN DE FIRMAS

	NOMBRE	CARGO
ELABORO:	Javier Parra Pinzón	ASSD Gestor del documento
REVISO:	Yudyett Astrid Pulido Guevara	Sistemas Integrados de Gestión – OAP.
APROBO:	Lady Paola Cuevas Triviño	Coordinador Grupo Gestión TIC (E)
	Coronel John Fredy Ubaque Rodríguez	Subdirector General, encargado de las funciones de Jefe Oficina Asesora de Planeación
	Dra. Elva Consuelo Cristancho Cristancho	Jefe Oficina Asesora Jurídica (E)
	Coronel John Fredy Ubaque Rodríguez	Subdirector General del Club Militar
FIRMANTE:	Contralmirante Javier Alfonso Jaimes Pinilla	Director General del Club Militar (E)

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL_03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2024

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20240131-190817-49de45-30357011 Creación: 2024-01-31 19:08:17

Estado: Finalizado Finalización: 2024-01-31 20:15:14

Escanee el código para verificación

Aprobación: Coronel John Fredy Ubaque Rodríguez - Subdirector General, encargado de las funciones de Jefe Oficina Asesora de Planeación

Coronel JOHN FREDY UBAQUE RODRIGUEZ
11189710
asistenteplaneacion@clubmilitar.gov.co
Subdirector General encargado de las funciones de Jefe Oficina Asesora de P
CLUB MILITAR

Aprobación: Lady Paola Cuevas Triviño - Coordinador Grupo Gestión TIC (E)

Lady Paola Cuevas
1030589228
lpcuevas@clubmilitar.gov.co
Técnico para seguridad apoyo y defensa
Club Militar

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

Yudyett Pulido
52915896
yapulido@clubmilitar.gov.co

Elaboración: Javier Parra Pinzón - ASSD Gestor del documento

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

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PL_03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2024

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20240131-190817-49de45-30357011
Creación: 2024-01-31 19:08:17
Estado: Finalizado
Finalización: 2024-01-31 20:15:14

Escanee el código para verificación

Firma: Contralmirante Javier Alfonso Jaimes Pinilla - Director General del Club Militar (E)

Contralmirante JAVIER ALFONSO JAIMES PINILLA
72170207
asistentedireccion@clubmilitar.gov.co
Director General (E)
Club Militar

Aprobación: Coronel John Fredy Ubaque Rodríguez - Subdirector General del Club Militar

CORONEL JOHN FREDY UBAQUE RODRÍGUEZ
1111
asistentesubdireccion@clubmilitar.gov.co
Subdirector General

Aprobación: Dra. Elva Consuelo Cristancho Cristancho - Jefe Oficina Asesora Jurídica (E)

Elva Consuelo Cristancho Cristancho
46372713
eccristancho@clubmilitar.gov.co
Profesional de Defensa
Club Militar

REPORTE DE TRAZABILIDAD

CM-GTI-PL_03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CLUB MILITAR 2024

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20240131-190817-49de45-30357011 Creación: 2024-01-31 19:08:17

Estado: Finalizado Finalización: 2024-01-31 20:15:14

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Javier Parra Pinzon jparra@clubmilitar.gov.co ASSD Club Militar	Aprobado	Env.: 2024-01-31 19:08:17 Lec.: 2024-01-31 19:11:35 Res.: 2024-01-31 19:12:01 IP Res.: 200.91.222.50
Revisión	Yudyett Pulido yapulido@clubmilitar.gov.co	Aprobado	Env.: 2024-01-31 19:12:01 Lec.: 2024-01-31 19:12:14 Res.: 2024-01-31 19:12:29 IP Res.: 200.91.222.50
Aprobación	Lady Paola Cuevas lpcuevas@clubmilitar.gov.co Técnico para seguridad apoyo y defensa Club Militar	Aprobado	Env.: 2024-01-31 19:12:29 Lec.: 2024-01-31 19:15:15 Res.: 2024-01-31 19:15:21 IP Res.: 200.91.222.50
Aprobación	Coronel JOHN FREDY UBAQUE RODRIGUEZ asistenteplaneacion@clubmilitar.gov.co Subdirector General encargado de las fun CLUB MILITAR	Aprobado	Env.: 2024-01-31 19:15:21 Lec.: 2024-01-31 19:29:06 Res.: 2024-01-31 19:55:33 IP Res.: 200.91.249.34
Aprobación	Elva Consuelo Cristancho Cristancho eccristancho@clubmilitar.gov.co Profesional de Defensa Club Militar	Aprobado	Env.: 2024-01-31 19:55:33 Lec.: 2024-01-31 19:57:17 Res.: 2024-01-31 19:57:26 IP Res.: 186.84.88.206
Aprobación	CORONEL JOHN FREDY UBAQUE RODRÍGUEZ asistentesubdireccion@clubmilitar.gov.co Subdirector General	Aprobado	Env.: 2024-01-31 19:57:27 Lec.: 2024-01-31 19:58:13 Res.: 2024-01-31 19:59:25 IP Res.: 200.91.249.34
Firma	Contralmirante JAVIER ALFONSO JAIMES asistentedireccion@clubmilitar.gov.co Director General (E) Club Militar	Aprobado	Env.: 2024-01-31 19:59:25 Lec.: 2024-01-31 20:01:11 Res.: 2024-01-31 20:15:14 IP Res.: 200.91.222.50