ClubMilitar
¡Actitud, Perseverancia y Pasión!

POLÍTICA DE ACCESO REMOTO VPN

TABLA DE CONTENIDO

INTRODUCCIÓN

El Club Militar considera que la información es un activo fundamental para el desarrollo de sus actividades, en razón a que es una herramienta de gran importancia para la toma de decisiones, motivo por el cual, el Grupo de Gestión TIC está comprometido en proteger los activos de información de la entidad (empleados, información documental tanto física como digital y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, pasantes y personal que hagan uso de los activos de información del Club Militar; siguiendo las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC y la norma NTC ISO 27001:2022.

Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones. El Club Militar busca a través de esta política apoyar los procesos de modernización organizacional, el aumento en la productividad, la mejora en la calidad de los servicios, la reducción de costos, el mejor empleo de los recursos institucionales, la inclusión social, el equilibrio entre la vida laboral y personal de los trabajadores, la movilidad urbana y la protección al medio ambiente.

1. POLÍTICA DE ACCESO REMOTO VPN

El Club Militar establece una política de acceso remoto VPN con el fin de regular la gestión de la seguridad de la información al interior y exterior de la entidad. Este documento relaciona los lineamientos y aspectos transversales de seguridad relacionados con la política de seguridad y privacidad de la información y las mejores prácticas que permiten a la entidad acceder y administrar de manera segura los servicios relacionados con el acceso remoto VPN.

Es muy importante para el Club Militar contar con esta política, ya que guiara el comportamiento personal y profesional sobre la información capturada, integrada y dispuesta desde un acceso remoto al interior y exterior de la entidad, así mismo permitirán al Club Militar trabajar bajo las mejores prácticas de seguridad y facilitará el cumplimiento de los requisitos legales a los cuales esté obligado en torno a esta materia.

Lo anterior, busca generar el uso adecuado de las tecnologías de la información, asignando permisos, generando autenticaciones y conexiones seguras de acuerdo con la sensibilidad de la información por acceder, verificando los aspectos de seguridad física, del entorno y el suministro de elementos tecnológicos.

2. OBJETIVO GENERAL

Definir los lineamientos para gestionar el acceso a los recursos de TIC del Club Militar mediante la conexión de Redes Virtuales Privadas (VPN), que permitan propender los principios de confidencialidad, integridad y disponibilidad de la información del Club Militar.

3. ALCANCE DE LA POLÍTICA

Abarca a todos los funcionarios (servidores públicos y/o trabajadores oficiales), contratistas, pasantes, personal en comisión, visitantes y proveedores externos que presten sus servicios o personal tenga algún tipo de relación con el Club Militar y que, a raíz de sus funciones, tenga la necesidad de realizar diversos accesos a los sistemas físicos y lógicos que la entidad posea,

incluyendo los archivos de documentación, las aplicaciones comerciales, las bases de datos, las aplicaciones desarrolladas internamente, los equipos, las instalaciones, los sistemas y las redes.

Esta política considera a todos los procesos operacionales, de apoyo y estratégicos que requieran en cualquiera de sus etapas la aplicación de controles de acceso tanto lógico como físicos.

Asimismo, esta incluye a todos los activos de información que el Club Militar posee, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger activos de información que se encuentren en otras formas. Así, esta política cubre toda la información impresa o soporte en papel, la almacenada electrónicamente, la trasmitida por correo u otro medio electrónico, la mostrada en películas o la utilizada en una conversación.

4. GLOSARIO

Cifrado de datos	Procedimiento que emplea un algoritmo de cifrado con cierta clave para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta del algoritmo.
Dispositivo de red	Cualquier hardware que conecte diferentes recursos de red, permitiendo la comunicación e interacción entre dos o más dispositivos.
Directorio Activo	Base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que se necesitan para ingresar a las diversas aplicaciones de la entidad a gestionar su trabajo.
DDos - Distributed Denial Of Service	Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
Red	Interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado.
Red LAN - Local Área Network	Red de Área Local, es un grupo de computadoras y dispositivos periféricos que comparten una línea de comunicaciones común o un enlace inalámbrico a un servidor dentro de un área geográfica específica.
RDP - Remote Desktop Protocol	Permite que el escritorio de un equipo informático sea controlado a distancia por un usuario remoto.
VPN - Virtual Private Network	Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando internet.
Usuario	Toda persona que tiene acceso a cualquier recurso tecnológico de la Agencia (correo electrónico, cuenta de dominio, bases de datos, aplicaciones corporativas, página web, entre otras).

5. NORMATIVIDAD

CONPES 3854 de 2016	Política Nacional de Seguridad Nacional busca fortalecer, identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.
CONPES 3995 de 2020	Política Nacional De Confianza y Seguridad Digital "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital, de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías".
Decreto 338 de 2022	Establece los lineamientos generales para la gobernanza de seguridad digital, con el cual busca aunar y dinamizar el desarrollo legal, los avances técnicos, así como los conocimientos estatales y privados para fortalecer la ciberseguridad del país.
Directiva Presidencial 02 Del 24 De febrero De 2022	Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MINTIC).
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la Información y de los Datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581 de 2012	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
Modelo de Seguridad y Privacidad de la Información (MSPI)	Conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.
Norma técnica colombiana 27001:2022	Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).
Resolución 500 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.
Resolución 1519 del 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

6. NIVELES DE AUTORIDAD Y RESPONSABILIDAD DE LA POLÍTICA

El Club Militar cuenta con diferentes tipos de activos de información y todos los funcionarios, contratistas, pasantes y personal que tengan algún tipo de relación con la entidad deben velar por el buen uso de estos, a través de la definición y apropiación de los siguientes lineamientos:

- Todo el personal que tenga acceso a la información del Club Militar, es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir la política descrita; entre ellos están: servidores públicos, contratistas, proveedores, pasantes, terceros, convenios entre instituciones y visitantes.
- El Oficial de Seguridad de la Información del Grupo de Gestión TIC o quien haga sus veces, debe asumir la responsabilidad en el desarrollo e implementación de la política, debe velar por el cumplimiento de la política, debe orientar a todo el personal que tenga acceso a la información de la entidad, debe coordinar actividades de gestión de riesgos de seguridad y ciberseguridad, debe apoyar la identificación de controles y debe poner en contexto al Club Militar, de toda la gestión sobre seguridad y privacidad de la información.
- El Grupo de Gestión TIC, asumirá el rol recomendado por la norma ISO 27001:2022, denominado comité de seguridad de la información.
- El propietario de los activos de información tiene la responsabilidad de establecer la valoración de los activos, clasificación y respectivo etiquetado teniendo en cuenta el modelo de clasificación de la información del Club Militar, igualmente definir el nivel de protección requerido ante accesos no autorizados, pérdida de la confidencialidad, integridad o disponibilidad, realizar el respectivo etiquetado de la información teniendo en cuenta la clasificación definida, mantener actualizada la matriz de activos de información definida por el oficial de seguridad de la información o quien haga sus veces en temas de ciberseguridad, validando los controles de acceso asignado a los activos, identificar riesgos asociados con la seguridad y privacidad de la información en los procesos de los cuales es responsable o tienen participación y reportar oportunamente eventos o incidentes de seguridad y privacidad de la información.

7. CRITERIOS DE APLICACIÓN

El Club Militar solo proveerá a través del Grupo de Gestión TIC la habilitación del usuario dentro del sistema VPN, el cual no tiene costo alguno para el usuario. Ante cualquier costo que el usuario genere para hacer uso de este servicio, será de su exclusiva responsabilidad. Estos costos se pueden originar producto de la adquisición de un equipo de cómputo, la contratación de un servicio de internet o bien del soporte para instalación de software necesario.

7.1 ÁMBITO DEL SERVICIO

- Los funcionarios (servidores públicos y/o trabajadores oficiales), contratistas, pasantes, personal en comisión, visitantes y proveedores externos que presten sus servicios o personal que tenga algún tipo de relación con el Club Militar que deseen acceso VPN deben entregar al Grupo de Gestión TIC el FORMULARIO SOLICITUD DE ACCESO A SERVICIOS INFORMÁTICOS para validar la justificación de la solicitud y conceder el servicio.
- Para mayor nivel de detalle y seguridad, los funcionarios (servidores públicos y/o trabajadores oficiales), contratistas, pasantes, personal en comisión, visitantes y proveedores externos que presten sus servicios o personal que tenga algún tipo de relación con el Club Militar deben consultar la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA

INFORMACIÓN que el Grupo de Gestión TIC tiene publicada, en donde se definen todos los aspectos importantes para la implementación y gestión sobre seguridad y privacidad de la información de la operación mediante el acceso por VPN.

- Los funcionarios (servidores públicos y/o trabajadores oficiales), contratistas, pasantes, personal en comisión, visitantes y proveedores externos que presten sus servicios o personal que tenga algún tipo de relación con el Club Militar que posean acceso VPN tendrán el acceso limitado a las redes de la entidad de acuerdo con el rol a desempeñar dentro del Club Militar y los grupos previamente establecidos dentro del concentrador VPN. Esto se establece a partir del FORMULARIO SOLICITUD DE ACCESO A SERVICIOS INFORMÁTICOS entregado al momento de solicitar el servicio.
- El Club Militar solo proveerá la habilitación del usuario para el acceso remoto VPN. Esto quiere decir, que el usuario será responsable de contratar un servicio de internet, coordinar la instalación del software necesario y todo lo asociado para la adecuada utilización de esta.

7.2 ÁMBITO DE ATENCIÓN

- El soporte computacional para el acceso remoto VPN solo será brindado exclusivamente a personas pertenecientes al Club Militar y no a personas ajenas a ella o a terceros.

7.3 ACCESO A LAN

- El servicio VPN otorgará al usuario acceso seguro a la red LAN del Club Militar.
- El acceso de usuarios a la red LAN del Club Militar, a través de una conexión VPN, debe ser realizado única y exclusivamente utilizando el puerto habilitado para dicho fin.
- El puerto de acceso a la red LAN del Club Militar, debe ser habilitado por el administrador del servicio. Cada usuario solo podrá tener activa una solo conexión VPN.
- Una vez que hayan transcurrido 10 minutos de inactividad, los usuarios del sistema VPN serán automáticamente desconectados de la sesión. El usuario deberá iniciarse sesión nuevamente para volver a conectarse a la red de la entidad.

7.4 ACCESO SEGURO A SERVICIOS DE LA ENTIDAD Y TERCEROS

- A través del acceso remoto VPN se puede acceder a todos los servicios internos brindados a través de la red de datos del Club Militar.
- La dirección IP que el acceso remoto VPN asigna a los usuarios, permite acceder a los recursos y distintos servicios externos del Club Militar con los cuales se tiene convenio.

7.5 ACCESO SEGURO AL EQUIPO DE COMPUTO

- Si el usuario desea acceder a su equipo asignado por el Club Militar desde la red WAN en forma segura, este deberá utilizar el software de acceso remoto recomendado.
- Es necesario configurar previamente el servicio de escritorio remoto en el computador al cual se desea acceder, debido a que el servicio VPN por sí solo no habilita dicho acceso.

7.6 ALCANCE DE CONEXIÓN VPN

- Para garantizar el buen uso de la conexión VPN, los usuarios declaran conocer que sus equipos, ya sea institucional o personales, forman parte de una extensión de la red del Club Militar, por lo tanto, están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las dependencias de la entidad.
- Solo usuarios previamente autorizados podrán utilizar los beneficios del Sistema VPN, los que, además, serán los responsables del correcto uso del servicio de acceso remoto VPN.
- Las cuentas de usuario y soporte VPN son exclusivamente para uso personal y exclusivo, para quienes se les ha asignado dichos privilegios, por lo cual está estrictamente prohibido facilitar el acceso a terceras personas.

7.7 BUENAS PRÁCTICAS

- **Seguridad de entorno**

  Para evitar errores involuntarios o bien cometidos intencionalmente por terceras personas que por descuido puedan ocupar la conexión VPN asignada, los cuales pueden ser nefastos tanto para el usuario como para el Club Militar, es necesario tener en cuenta lo valioso que puede ser el hecho de realizar las siguientes actividades:

- Es importante tener en cuenta que la contraseña de autenticación asignada nunca deberá ser divulgada a terceros, y siempre debe ser mantenida en secreto, lo cual garantiza el uso personalizado y correcto del sistema VPN, y a su vez resguarda el uso de información personal.
- Configurar el protector de pantalla y la contraseña de entrada del equipo donde instalará la VPN, de forma que, si deja libre por un momento su estación de trabajo, otra persona no tendrá acceso a los recursos del Club Militar.
- Desconectar la VPN una vez concluida las operaciones a realizar en la red del Club Militar.

7.8 CAMBIO DE CLAVE

- Para solicitar un cambio de clave, el usuario debe comunicarse con el Grupo de Gestión TIC vía correo electrónico o bien a través de la herramienta TIC-atento: http://200.91.222.50:8086/mesadeayuda.

7.9 CLAVES VPN

Asignación de clave

- Para garantizar el uso personalizado del acceso remoto VPN, se asigna una contraseña de autenticación, la cual nunca deberá ser divulgada, siempre debe ser mantenida en secreto.

Pérdida de clave

- Si el usuario olvida la clave de su cuenta VPN, debe enviar un correo al Grupo de Gestión TIC informado de la situación o mediante la herramienta TIC-atento: http://200.91.222.50:8086/mesadeayuda, ante lo cual se generará una nueva contraseña.

7.10 DISPONIBILIDAD DEL SERVICIO

- El horario habilitado para la conexión VPN a la red del Club Militar para usuarios está establecido de lunes a sábado de 6:00 a 22:00 horas y para usuarios que tengan el rol de soporte es permanente 24/7. Solo en casos particulares

y mediante solicitud previa con su respectiva justificación, el Grupo de Gestión TIC permitirá el acceso VPN para usuarios en un horario 24/7; el cual no deberá estar en un estado permanente, sino en un estado temporal bajo supervisión constante.

7.11 ELIMINACIÓN DE CUENTAS VPN

- **Eliminación por solicitud**

  Si el usuario por alguna razón desea eliminar su cuenta VPN, debe solicitar dicho procedimiento a través del FORMULARIO SOLICITUD DE ACCESO A SERVICIOS INFORMÁTICOS.

- **Eliminación por inactividad**

  Si el usuario no ha utilizado su cuenta de acceso VPN en un periodo de tiempo de 11 meses consecutivos, el Grupo de Gestión TIC le informará vía correo electrónico que su cuenta queda suspendida por tal motivo.

  Si el usuario no responde al aviso realizado en el onceavo mes, al cumplirse el año de inactividad, inmediatamente la cuenta queda eliminada del sistema.

  Si el usuario desea tener nuevamente una cuenta VPN, deberá volver a realizar la solicitud a través del FORMULARIO SOLICITUD DE ACCESO A SERVICIOS INFORMÁTICOS.

- **Eliminación por desvinculación de la entidad**

  Si el usuario ha sido desvinculado del Club Militar, su cuenta de acceso VPN será caducada automáticamente.

7.12 RESGUARDO DE LA INFORMACIÓN

- Un usuario al momento de ingresar al dominio del Club Militar a través de internet, debe tener la claridad que desde ese momento se podrá conectar a todos los recursos disponibles en la LAN de la entidad, o bien para decirlo de manera más específica, también el usuario podrá conectarse a un computador residente en las oficinas del Club Militar. Por lo tanto, todos los recursos alcanzables por una conexión VPN, como son Bases de Datos personales, Bases de Datos corporativas, correos electrónicos, documentos residentes en carpetas compartidas o bien en unidades remotas, se pueden ver afectados por un descuido o mal uso.
- Se recomienda tomar los resguardos necesarios conducentes a conservar la integridad de la información a la cual se tenga acceso, para eso se deben tomar las debidas precauciones de conexión y desconexión recomendadas por esta el Grupo de Gestión TIC en su documento POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
- Independiente del buen uso que se le dé al servicio VPN, es conveniente realizar respaldos periódicos de toda la información que está bajo su responsabilidad, como pueden ser bases de datos, informes, etc.
- Esta aplicación solo debe ser instalada en equipos que estén bajo responsabilidad de personas que tengan algún tipo de vínculo contractual con el Club Militar, por consiguiente, el Grupo de Gestión TIC validará el estatus de la persona solicitante.
- La aplicación necesaria para dar acceso remoto VPN no debe ser instalada en equipos de uso público.

7.13 SITUACIONES ESPECIALES

- **Pérdida de equipo**

En el caso de que un usuario sufra el robo de su equipo personal, debe informar cuanto antes al Grupo de Gestión TIC para qué la cuenta VPN asignada sea bloqueada. Luego de esto, si el usuario lo solicita, se generará una nueva cuenta.

- **Ingreso no autorizado por un tercero**

  En el caso de que un usuario detecte que una persona no autorizada haya utilizado su cuenta VPN, debe dar aviso cuanto antes al Grupo de Gestión TIC, para analizar los pasos a seguir según cada caso particular.

7.14 SOPORTE

- Ante cualquier problema que presente el uso del sistema, se debe informar al personal del Grupo de Gestión TIC, quienes se encargarán de buscar una solución a dicho problema.
- **Horarios de atención soporté**

  La atención de consultas, junto con las distintas actividades de mesa de ayuda relativa al sistema, se realizarán en los siguientes horarios:

Días	Horario de atención
Lunes a viernes	8:30 a 17:00
Sábado	8:30 a 16:00

- Una vez recibida la solicitud, los tiempos de respuesta máximos de atención definidos son de 24 horas.

7.15 VULNERACIÓN DE POLÍTICAS

- Los usuarios que sean sorprendidos vulnerando o intentando vulnerar las políticas impuestas por el Club Militar, se bloqueará inmediatamente el acceso al servicio y se iniciará el proceso para determinar su sanción.

8 CONTROL DE CAMBIOS

Versión	Fecha del cambio	Descripción de la actualización
1	24/11/2022	Creación de documento
2	18/09/2023	Actualización de documento al nuevo formato junto con su normativa y ampliación específica del contenido de la política para su alineación con la política de seguridad y privacidad de la información del Club Militar.

9 VALIDACIÓN DE FIRMAS

ELABORÓ	REVISÓ	APROBÓ
Firma Nombre: ING **ADRIAN RICARDO GELVES ANGARITA** Cargo: Apoyo del Grupo de Gestión TIC	Firma Nombre: ING **NELSON DARÍO FLÓREZ GARCÍA** Cargo: Coordinador Grupo de Gestión TIC Firma Nombre: CR **JOHN FREDY UBAQUE RODRÍGUEZ** Cargo: Subdirector General, encargado de las funciones de Jefe de la Oficina Asesora de Planeación Firma Nombre: DRA **ELVA CONSUELO CRISTANCHO CRISTANCHO** Cargo: Encargado de las funciones de Jefe Oficina Asesora Jurídica Firma Nombre: CR **JOHN FREDY UBAQUE RODRÍGUEZ** Cargo: Subdirector General	Firma Nombre: VA (RA) **HÉCTOR ALFONSO MEDINA TORRES** Cargo: Director General

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PO-01 POLÍTICA DE ACCESO REMOTO VPN

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20230927-092424-141e23-25109922 Creación: 2023-09-27 09:24:24
Estado: Finalizado Finalización: 2023-10-10 14:54:08

Escanee el código para verificación

Revisión: REVISIÓN - CR JOHN FREDY UBAQUE RODRÍGUEZ

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

Revisión: REVISIÓN - ING NELSON DARIO FLOREZ GARCIA

Nelson Florez
80390968
ndflorez@clubmilitar.gov.co

Elaboración: ELABORACIÓN - ING ADRIAN RICARDO GELVES ANGARITA

Adrian Ricardo Gelves Angarita
1094279950
argelves@clubmilitar.gov.co
Apoyo en Grupo de Gestión TIC
Club Militar

Notificacion: NOTIFICACIÓN - YUDYETT ASTRID PULIDO GUEVARA

Yudyett Pulido
52915896
yapulido@clubmilitar.gov.co

REGISTRO DE FIRMAS ELECTRONICAS

CM-GTI-PO-01 POLÍTICA DE ACCESO REMOTO VPN

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20230927-092424-141e23-25109922
Creación: 2023-09-27 09:24:24
Estado: Finalizado
Finalización: 2023-10-10 14:54:08

Escanee el código para verificación

Aprobación: APROBACIÓN - VA (RA) HÉCTOR ALFONSO MEDINA TORRES

Vicealmirante (RA) HÉCTOR ALFONSO MEDINA TORRRES
73126706
asistentedireccion@clubmilitar.gov.co
Director General
Club Militar

Revisión: REVISIÓN - CR JOHN FREDY UBAQUE RODRÍGUEZ

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

Revisión: REVISIÓN - DRA ELVA CONSUELO CRISTANCHO CRISTANCHO

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

REPORTE DE TRAZABILIDAD

CM-GTI-PO-01 POLÍTICA DE ACCESO REMOTO VPN

Club Militar
gestionado por: azsign.com.co

Id Acuerdo: 20230927-092424-141e23-25109922 Creación: 2023-09-27 09:24:24
Estado: Finalizado Finalización: 2023-10-10 14:54:08

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Notificacion	Yudyett Pulido yapulido@clubmilitar.gov.co	Aprobado	Env.: 2023-09-27 09:24:24 Lec.: 2023-09-27 09:31:13 Res.: 2023-09-27 09:32:11 IP Res.: 200.91.222.50
Elaboración	Adrian Ricardo Gelves Angarita argelves@clubmilitar.gov.co Apoyo en Grupo de Gestión TIC Club Militar	Aprobado	Env.: 2023-09-27 09:32:11 Lec.: 2023-09-27 09:35:13 Res.: 2023-09-27 09:35:45 IP Res.: 200.91.222.50
Revisión	Nelson Florez ndflorez@clubmilitar.gov.co	Aprobado	Env.: 2023-09-27 09:35:45 Lec.: 2023-09-27 09:39:04 Res.: 2023-09-27 09:41:48 IP Res.: 200.91.222.50
Revisión	Coronel JOHN FREDY UBAQUE RODRIGUEZ asistenteplaneacion@clubmilitar.gov.co Subdirector General encargado de las fun CLUB MILITAR	Aprobado	Env.: 2023-09-27 09:41:48 Lec.: 2023-09-27 10:21:56 Res.: 2023-09-27 18:40:07 IP Res.: 200.91.249.34
Revisión	Elva Consuelo Cristancho Cristancho eccristancho@clubmilitar.gov.co Profesional de Defensa Club Militar	Aprobado	Env.: 2023-09-27 18:40:07 Lec.: 2023-09-28 11:58:44 Res.: 2023-09-28 11:58:59 IP Res.: 200.91.222.50
Revisión	CORONEL JOHN FREDY UBAQUE RODRÍGUEZ asistentesubdireccion@clubmilitar.gov.co Subdirector General	Aprobado	Env.: 2023-09-28 11:58:59 Lec.: 2023-09-28 13:28:18 Res.: 2023-09-29 17:02:54 IP Res.: 200.91.249.34
Aprobación	Vicelamirante (RA) HÉCTOR ALFONSO MED asistentedireccion@clubmilitar.gov.co Director General Club Militar	Aprobado	Env.: 2023-09-29 17:02:54 Lec.: 2023-10-02 10:32:31 Res.: 2023-10-10 14:54:08 IP Res.: 200.91.249.34