TABLA DE CONTENIDO

INTRODUCCIÓN

El Club Militar, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

La política de seguridad y privacidad de la información del Club Militar tiene como principio fundamental la implementación de controles, procesos y estándares para garantizar la disponibilidad, integridad y disponibilidad de los activos de información, enmarcados en el modelo de Gobierno y Seguridad Digital.

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DEL NEGOCIO

El Club Militar adopta el Modelo de Seguridad y Privacidad de la Información, adquiriendo el compromiso de organizar, planificar, implementar, soportar, operar, evaluar y mejorar la Seguridad de la Información de la entidad, con el fin de proteger, preservar y asegurar la integridad, confidencialidad y disponibilidad de los activos de información que soportan los procesos administrativos y operativos del Club Militar.

2. OBJETIVO GENERAL

Definir una Política de Seguridad de la Información para el Club Militar que refleje los procesos y procedimientos que se llevan a cabo a nivel de Tecnologías de la Información y Comunicaciones, garantizando la integridad, confidencialidad y disponibilidad de la seguridad de la información.

3. OBJETIVOS ESPECIFICOS

- Establecer y vigilar el cumplimiento de los principios mínimos declarados en esta política para garantizar la seguridad y privacidad de la información.
- Asegurar la existencia de controles y procedimientos que orienten a la satisfacción de la propuesta presentada.

- Evaluar las acciones que lleven a cabo para actualizar los diferentes procesos a nivel de usuario, red y Seguridad de la Informática.
- Verificar parámetros de medición de desempeño en el área de sistemas.

4. ALCANCE DE LA POLÍTICA

La Política de seguridad y privacidad de la información del Club Militar aplica a todos los funcionarios e instancias de la entidad (Directivo, administrativo, operativo y otros terceros que desempeñan alguna actividad o labor dentro de las instalaciones del Club Militar)

5. GLOSARIO

- **Activo Informático:** Cualquier cosa que tiene valor para la organización en el campo informático. En este concepto se incluyen la información, todo el Hardware y Software, e infraestructura de redes y comunicaciones, tales como equipos de cómputo o para procesamiento de información, sistemas operativos, bases de datos, sistemas de almacenamiento masivo de información, aplicaciones, programas, sistemas de información, dispositivos de comunicaciones alámbricas e inalámbricas y dispositivos y accesorios relacionados con todos los anteriores así como los dispositivos para control de acceso físico y lógico y para seguridad informática.

- **Administrador:** Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo.

- **Amenazas Informáticas:** Eventos que pueden desencadenar un incidente informático en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. La amenaza se puede materializar y transformarse en agresiones. Puede afectar confidencialidad, integridad y disponibilidad de los sistemas de información. Existen amenazas relacionadas con falla humanas, con ataques malintencionados o con catástrofes naturales. Mediante la materialización de una amenaza podría ocurrir el acceso modificación o eliminación de información no autorizada; la interrupción de un servicio o el procesamiento de un sistema; daños físicos o robo del equipamiento y medios de almacenamiento de información, entre las principales amenazas tenemos Ingeniería Social, Phishing, Escaneo de Puertos, Wardialers, Código Malicioso (Virus), Exploits, Ataques de Contraseña, Control Remoto de Equipos, Man-in-the-middle, Defacement, IP Spoofing - MAC Address Spoofing, entre otros.

- **Análisis De Riesgo:** El riesgo es usualmente vinculado a la probabilidad de que ocurra un evento no deseado generalmente la probabilidad de que ocurra dicho evento y algún asesoramiento sobre el daño que se espera de él deben ser unidos en un escenario creíble que combine el riesgo y las probabilidades de

arrepentimiento y recompensa en un valor esperado. Hay muchos métodos informales que se usan para asesorar sobre el riesgo (o para "medirlo", aunque esto no suele ser posible) y otros formales.

- En el análisis de escenarios el "riesgo" es distante de lo que se llama "amenaza". Una amenaza es un evento serio pero de poca probabilidad - pero cuya probabilidad puede no ser determinada por algunos analistas en un asesoramiento de riesgo porque nunca ha ocurrido, y para la cual ninguna medida preventiva está disponible. La diferencia está más claramente ilustrada por el principio de precaución que busca disminuir la amenaza reduciéndola a una serie de riesgos bien definidos antes de que un acción, manual, innovación o experimento sea llevado a cabo. En seguridad de la información (se llamará así a la protección de cualquier tipo de información, no solo a la los sistemas informáticos) el riesgo es definido como la función de tres variables: la probabilidad de que haya una amenaza, de que haya debilidades y el impacto potencial.

- **Análisis De Vulnerabilidades:** Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.

- **Antena:** Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia qué punto emitan la señal podemos encontrarlas direccionales u omnidireccionales.

- **Anti-Virus:** Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos.

- **Antispam:** Equipo dedicado o software que mediante una serie de reglas y filtros, busca identificar correos publicitarios no deseados (spam) para evitar llenar el buzón y evitar pérdida de tiempo en la revisión de éstos. Los equipos antispam se valen de diferentes tipos de filtros, como las listas negras, los bayesianos, entre otros.

- **Antispyware:** Equipo dedicado o software que detecta y elimina el spyware detectado, así como previene la instalación de nuevo spyware. Los equipos antispyware al reconocer un equipo infectado, evitan las acciones que realiza el spyware, así como el envío de información privada, que el spyware se extienda en otros equipos.

- **Archivo:** Conjunto de bytes relacionados y tratados como una unidad. Un archivo puede contener programas, datos o ambas cosas.

- **Ataque:** Intento de comprometer alguna de las capacidades de un sistema de información. Dependiendo del objetivo del ataque, pueden afectar a la confidencialidad, integridad o disponibilidad del sistema. El ataque puede ser un evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

- **Atacante:** Son las personas que buscan tener acceso ilegal a los activos informáticos de una organización. En este rol se pueden distinguir tres tipos hacker, cracker y lammer:

- **Ataques Pasivos:** Ataques que se limitan a acceder de forma no autorizada a información protegida. Este tipo de ataque no afecta los parámetros de configuración del sistema ó los datos. Básicamente ataca la confidencialidad del sistema de información.

- **Ataque Activo:** Ataque al sistema para insertar información falsa o corromper la ya existente. Este ataque afecta los tres requerimientos de la seguridad: confidencialidad, integridad y disponibilidad.

- **Ataques A Passwords - Password Attacks:** Es un intento de obtener o descifrar una password legítima de usuario. Las medidas de seguridad contra estos ataques son muy limitada consistiendo en una política de passwords, que incluye una longitud mínima, palabras no reconocibles y cambios frecuentes.

- **Ataque De Fuerza Bruta - Brute Force Attack:** Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas). Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.
- **Auditabilidad:** Cuando la información relacionada con las acciones y actividades de los usuarios (personas o procesos) se encuentra debidamente registrada y monitoreada. P.e.: Logs de las transacciones que un usuario ha realizado en un sistema determinado

- **Auditor:** Son generalmente personas externas a la organización que realizan revisiones a la seguridad implantada y realizan recomendaciones para su mejoramiento. Son personas de apoyo para el administrador de seguridad porque le pueden dar consejos de implantaciones de seguridad, hacerlo caer en la cuenta de falencias de seguridad y apoyarlo en nuevos diseños e implantaciones al respecto.

- **Auditoría:** Análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos. Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.

- **Autorización:** Proceso por el que se acredita a un sujeto o entidad, para realizar una acción determinada. Se dice que hay autorización cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo. Ejemplo: perfiles de usuario en las aplicaciones.

- **Autenticidad:** Propiedad fundamental de la información de ser confrontada en cualquier momento de su ciclo de vida contra su origen real (Verdadero/falso). Especialmente importante en sistemas económicos (banca, comercio electrónico, bolsa de valores, apuestas, etc.)

- **Backup**: Es una réplica de datos que nos permite recuperar la información en caso de ser necesario. Hacer un backup, consiste en guardar en un medio extraíble (para poder guardarlo en lugar seguro) la información sensible referida a un sistema. Esta se puede realizar tanto en ordenadores personales como en servidores. Este medio puede ser un disco duro externo, un CD-ROM grabable, cintas de datos (DAT), discos ZIP o JAZ o magneto-ópticos ó cualquier otro dispositivo de almacenamiento.

- **Base De Datos:** Es un conjunto de datos estructurados que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso.

- **Biométricos:** Son elementos electrónicos que mediante la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, pueden "verificar" identidades o "identificar" individuos.

- **BIT:** El bit es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información. Con él, podemos representar dos valores cualesquiera, como verdadero o falso, abierto o cerrado. Basta con asignar uno de esos valores al estado de "apagado" (0), y el otro al estado de "encendido" (1).

- **BYTE:** Combinación de Bits. En la representación más común 8 bits forman un byte.

- **Caballo De Troya**: Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño. Véase también Troyano.

- **Cableado Eléctrico:** Circuito eléctrico o electrónico que exige el montaje de distintos módulos unidos (cableados) entre sí, para realizar un determinado proceso o secuencia lógica, que por lo general servirá para controlar un sistema de potencia.

- **Clave:** Palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc. Véase Contraseña - Password.

- **Código Fuente:** Un programa escrito en un formato entendible por el hombre pero no por la computadora. Necesita ser "traducido" (Compilar) a código máquina para ser interpretado por esta última.

- **Código Malicioso / Virus:** Se define como todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Existen diferentes tipos de código malicioso; a continuación, mencionamos algunos de ellos bombas lógicas, troyanos, gusanos, Keyloggers, Cookies, Spyware.

- **Confidencial:** Tipo de clasificación de la información que por su contenido solo interesa a quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios a determinada entidad, agrupación o persona. Se incluyen en esta los siguientes documentos:
  Estudio de Seguridad de Personal (ESP).
  Hojas de vida.
  Historial de personal.
  Información de carácter personal.

- **Confidencialidad:** Requisito de seguridad que indica que el acceso a los recursos de sistema debe estar limitado exclusivamente a los usuarios con acceso autorizado.

- **Contingencia:** Es la posibilidad de algo suceda. Lo que puede o no suceder. Las contingencias de orden natural o humano, deben ser previstas mediante un plan que describa la aplicación de medidas técnicas, humanas y organizativas que garanticen la continuidad de las operaciones de la Entidad.

- **Contraseña – Password:** Conjunto de caracteres alfanuméricos y símbolos que forman una serie secreta de que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa. En sistemas multiusos, cada usuario debe incorporar su contraseña antes de que el ordenador responda a los comandos. Las contraseñas ayudan a asegurar que los usuarios desautorizados no tengan acceso al ordenador. Además, los ficheros de datos y los programas pueden también requerir contraseñas.

- **Control De Accesos - Access Control:** Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, mainframes, Internet, ftp, web. El permiso o la denegación de acceso pueden realizarse en función de la dirección IP, el nombre de dominio, nombre de usuario y password, certificados.

- **Control Remoto De Equipos:** Un atacante puede tomar el control de un equipo en forma remota y no autorizada, mediante la utilización de programas desarrollados para tal fin, e instalados por el atacante mediante, por ejemplo la utilización de troyanos.

- **Correo Electrónico (E-Mail) :** Aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. También denominado E-Mail.
- **Delito Informático - Computer Crime:** Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

- **Detección De Intrusos (Ids):** Sistema que agrupa un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema.

- **Detección De Intrusiones:** Proceso de monitorizar los eventos de un sistema o red en busca de signos que indiquen problemas de seguridad.

- **Detección De Usos Indebidos:** Detección basada en la actividad de sistema que coincide con la definida como mala.

- **DHCP –(Dynamic Host Configuration Protocol):** Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuánto tiempo la ha tenido, a quien se la ha asignado después.

- **Disponibilidad:** Requisito de seguridad que implica que la información y los servicios del sistema continúen en funcionamiento y que los usuarios autorizados puedan acceder a los recursos cuando lo necesiten, dónde lo necesiten, y en la forma en que lo necesiten.

- **Dispositivo Móvil (DM) - Mobile Device:** Dispositivo electrónico cuya función es la de recibir/enviar información desde la estación en que esté instalado (portátiles, PDAs, móviles, cámaras, impresoras,). Este dispositivo puede ser una tarjeta PCMCIA, USB, PCI -Slot de un PC de sobremesa-, ó Centrino, que sustituyen a las tarjetas de red.

- **Estándar:**Conjunto de requisitos de obligatorio cumplimiento, que especifican tecnologías y métodos, para implementar las políticas de seguridad informática expuestas por la alta gerencia, establecen un marco de

acción coordinado que busca alinear los esfuerzos de la organización para procurar los fundamentos de la seguridad informática.

- **Ethernet :** Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. en cooperación con DEC e Intel que. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps. Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.

- **Escaneo De Puertos:** Consiste en detectar qué servicios posee activos un equipo, con el objeto de ser utilizados para los fines del atacante.

- **Extranet:** Red privada virtual resultante de la interconexión de dos o más intranets que utiliza Internet como medio de transporte de la información entre sus nodos.

- **Firewall:** Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de la información.

- **Forense:** Personas expertas que se encargan de realizar análisis de siniestros de seguridad ocurridos dentro de la organización para determinar lo que paso y quién lo hizo, y si es el caso, aportar en procesos penales contra los atacantes

- **Fraude Informático:** Se trata del perjuicio económico efectuado a una persona mediante la utilización de un sistema informático, ya sea, modificando datos, introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee la seguridad del sistema.

- **FTP:** Es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Ficheros) y es el ideal para transferir grandes bloques de datos por la red.

- **Gateway:** Dispositivo de enrutamiento. En la actualidad, se utiliza el término Router para describir los nodos que realizan esta función, mientras que Gateway se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro.

- **Gestión De Seguridad:** Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución. 2. En gestión de redes, controlar (permitir, limitar, restringir, o denegar) acceso a la red y recursos, buscar intrusiones, identificar puntos de entrada de intrusiones, y reparar o cerrar estas posibles vías de acceso.

- **Gusano:** Es un virus o programa auto replicante que no altera los archivos, sino que reside en la memoria y se duplica a sí mismo.

- **Hacker:** Son personas expertas en sistemas que saben de seguridad que lo que buscan es tener acceso a recursos informáticos generalmente con el fin de demostrarse a sí mismo y a otros que lo pudieron hacer y conseguir prestigio como expertos en seguridad.

- **Hardware:** Se denomina hardware o soporte físico al conjunto de elementos materiales que componen un computador. Hardware también son los componentes físicos de una computadora tales como el disco duro, CD-Rom, disquetera (floppy). En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

- **Hash:** Un valor hash, también conocido como "message digest", es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.

- **Host:** Sistema Central. Computadora que permite a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el Correo Electrónico, Telnet y FTP.

- **HTML - Hypertext Markup Language):** Lenguaje de marcas hipertextuales. Lenguaje de marcación diseñado para estructurar textos y presentarlos en forma de hipertexto, que es el formato estándar de las páginas web, formato especial de archivos sobre el que está basada la estructura de la aplicación WWW (World Wide Web).

- **HTTP -(Hypertext Tranfer Protocol):** El protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares.

- **ID:** Conjunto de caracteres alfanuméricos que sirven para Identificar a un usuario para su acceso a la red o un sistema de información. Ej: rfgarcia.

- **IDS:** Intrusión Detection System, es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, de Script Kiddies que usan herramientas automáticas.

- **Incidente Informático:** Cualquier acción, evento adverso o intento de ocurrencia de estos en un sistema o red informática que ponga en riesgo la confidencialidad, integridad y disponibilidad de la información.

- **Infraestructura:** Topología de una red inalámbrica que consta de dos elementos básicos: estaciones cliente wireless y puntos de acceso.

- **Ingeniería Social:** Consiste en utilizar artilugios, tretas y otras técnicas para el engaño de las personas logrando que revelen información de interés para el atacante, como ser contraseñas de acceso. Se diferencia del resto de las amenazas básicamente porque no se aprovecha de debilidades y vulnerabilidades propias de un componente informático para la obtención de información.

- **Integridad:** Requisito de seguridad que indica que la información deberá ser protegida ante alteraciones no autorizadas.

- **Intrusión:** Violación intencionada de las políticas de seguridad de un sistema.

- **Integridad De Archivos:** Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).

- **Internet:** Sistema de redes de computación ligadas entre si, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias.

- **Intranet:** Red de ordenadores de una red de área local (LAN) privada empresarial o educativa que proporciona herramientas de Internet, las cuales tienen como función principal proveer lógica de negocios para aplicaciones de captura, reportes, consultas.

- **Intruso:** Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software.

- **IP – Internet Protocol:** Protocolo de internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de internet. El IP es la dirección numérica de una computadora en internet, de forma que cada dirección electrónica se asigna a una computadora conectada a internet y por lo tanto es única. La dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI y está compuesta de cuatro octetos, como por ejemplo: 132.248.53.10 .

- **IPS:** Combinación de filtro (firewall) con un sistema de detección de intrusos IDS.

- **ISO:** Organización Internacional para la Estandarización.

- **ISO 17999:** Estándar para la gestión de la seguridad de la información.

- **ISO 27002:** Estándar que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información de una organización (Objetivos de control).

- **Keyloggers:** Es una aplicación destinada a registrar todas las teclas que un usuario tipea en su computador; algunos de ellos además registran otro tipo de información útil para un atacante, como ser, imágenes de pantalla.

- **LAN (Local Area Network):** Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Véase también MAN y WAN.

- **LOG:** Conjunto de archivos que contienen registros detallando todos los eventos relacionados con la seguridad de los recursos informáticos.

- **Login:** Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

- **Llaves Públicas:** Parte pública para criptografía que se entrega a quién se desea hacer un intercambio de información seguro.

- **Llaves Privadas:** Parte privada para criptografía que se no se entrega para hacer intercambio de información seguro y se utiliza para des encriptar la información encriptada con la llave pública.

- **MAC - Dirección De Control De Acceso A Medios:** Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexadecimal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.

- **MALWARE:** Este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos, spyware o incluso los bots, intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.

- **MAN(Metropolitan Area Network):** Red de área metropolitana. En general, una MAN abarca un área geográfica más vasta que una LAN, pero cubre un área geográfica más pequeña que una WAN.

- **Man-In-The-Middle:** Modalidad de ataque en que el atacante se interpone entre el origen y el destino en una comunicación pudiendo conocer y/o modificar el contenido de los paquetes de información, sin esto ser advertido por las víctimas. Esto puede ocurrir en diversos ambientes, como por ejemplo, en comunicaciones por e-mail, navegación en Internet, dentro de una red LAN.

- **No Repudio:** Característica de los sistemas de autenticación fuertes. Se da cuando la información involucrada en un evento corresponde a quien participa, quien no podrá evadir su intervención en éste. Ejemplo: Un emisor de un mensaje no puede negar que lo generó y viceversa, un receptor de un mensaje no puede negar que lo recibió.

- **Nodo:** Cualquier computadora o periférico conectado directamente a una red.

- **Norma:** Es una declaración organizacional que limita las responsabilidades entre diferentes áreas, estableciendo pautas de acción según lo que le correspondan en ámbito de sus funciones.

- **Online:** En general, se dice que algo está en línea, on-line u online si está conectado a una red o sistema mayor (que es, implícitamente, la línea).

- **OSI (Open System Interconection):** Lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

- **Patch (Parche):** Modificación de un programa ejecutable para solucionar un problema, corregir un Bug o para cambiar su comportamiento.

- **Perfil De Usuario:** Información a la que el usuario necesita acceder para el desarrollo de sus tareas, criticidad de la información, funciones del puesto.

- **Plan De Contingencia:** Definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización.

- **Políticas De Seguridad Informática:** Son directrices de nivel del Comando de las Fuerzas Militares en la cual se expresan valores y objetivos de la Institución para proporcionar dirección y soporte a los temas relacionados con seguridad informática.

- **Políticas De Uso Aceptable –Pua:** Normas que establecen el uso que se puede hacer de un activo informático o de una red en un ámbito dado. Las políticas de uso aceptable, para la red del Club Militar tienen como objetivo asegurar que toda la información existente de forma computarizada e impresa, este salvaguardada correctamente. También se proporcionan para asegurarse de que el proceso automatizado que involucra la colección, creación, manipulación, almacenamiento, recuperación, transmisión, y despliegue de la información este salvaguardado de manera apropiada dependiendo de su valor, contra destrucción, acceso no autorizado, modificación, sabotaje, hurto o fuga de información sensible y/o clasificada.

- **Procedimiento o Instructivo:** Define un conjunto de pasos operacionales específicos sugeridos para efectuar una labor particular, que se puede modificar en respuesta a los cambios en la dinámica del negocio y la tecnología. P.e Procedimiento para toma de respaldos.

- **Protocolo:** Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

- **Proxy:** Software que permite a varios ordenadores acceder a Internet a través de una única conexión física y puede permitir acceder a páginas WEB, FTP, correo electrónico, y también servidor de comunicaciones responsable de canalizar el tráfico entre una red privada e Internet, que contiene un cortafuego.

- **Puerto:** Punto de acceso a un ordenador ó medio a través del cual tienen lugar las transferencia de información – entradas / salidas - Todas las conexiones y diálogos TCP/IP se llevan a cabo sobre estos, y cada protocolo para su uso tiene definido un puerto estándar. En Internet, el término puerto se refiere a un número que se muestra en una URL, después de una coma justo después del Nombre de Dominio. Cada servicio en un servidor de Internet escucha en un número de puerto particular. La mayoría de estos servicios tienen números de puerto estándares. Los servidores web escuchan normalmente en el puerto 80, y el puerto Gopher estándar es el 70. (Los servicios pueden también escuchar en puertos no estándar, en cuyo caso el número de puerto se debe especificar en una URL cuando se acceda al servidor).

- **Red:** Conjunto de computadoras, impresoras, Routers, Switches, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.

- **Redundancia:** Consiste en intensificar y repetir la información o el servicio con el fin de tener una fuente alternativa en caso de daño del sistema principal.

- **Registros (Logs):** Registro oficial de eventos durante un periodo de tiempo en particular.

- **Reservado:** Tipo de clasificación de la Información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la institución militar, proporcionar ventajas a la amenaza actual o potencial, causar bajas o pérdidas propias en acciones de defensa nacional.

- **Restringido:** Tipo de clasificación de la Información que está dirigida a los miembros de la institución y que se debe proteger del conocimiento de personas extrañas a la misma.

- **Riesgo:** Es el daño potencial que puede surgir por un proceso presente o evento futuro. Diariamente en ocasiones se lo utiliza como sinónimo de probabilidad, pero en el asesoramiento profesional de riesgo, el riesgo combina la probabilidad de que ocurra un evento negativo con cuánto daño dicho evento causaría.

- **ROOT:** Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo. Véase también Administrador.

- **Router:** Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios host.

- **Secreto:** Tipo de de clasificación de Información pertinente a actividades o planes de defensa nacional interna o externa y operaciones de inteligencia relativa a la misma, cuya divulgación no autorizada podría afectar las relaciones diplomáticas, lesionar el prestigio del país o poner en peligro la estabilidad interna del mismo.

- **Seguridad Informática:** Disciplina cuyo objetivo es el estudio de los métodos y medios de protección frente a revelación, modificación, pérdida o destrucción de la información o ante fallos de procesos, almacenamiento o transmisión de dicha información. Principalmente se ocupa de garantizar la

confidencialidad, integridad y disponibilidad de la información frente a las amenazas y riesgos que afectan los sistemas de información.

- **Server (Servidor):** Máquina que ofrece servicios a otras dentro de una red. También llamado Host.

- **SFTP:** Es una versión segura de FTP. Toda la información intercambiada entre su ordenador y el servidor es encriptada, lo que quiere decir que los hackers no pueden interceptar sus comunicaciones y obtener así información como contraseñas.

- **Sistema De Gestión De La Información:** Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

- **Sistema Operativo:** Operating System (OS) en inglés. Programa especial el cual se carga en una computadora al prenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, MacOS son todos sistemas operativos.

- **SMTP -Simple Mail Transfer Protocol:** Protocolo que proporciona la capacidad de almacenamiento y reenvío del correo entre los Host de los sistemas de correo de la red.

- **Software:** Se denomina software (también programática, equipamiento lógico o soporte lógico) a todos los componentes intangibles de un ordenador o computadora, es decir, al conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).

- **SPAM:** Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.

- **Spyware:** Aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar de si el software que utiliza el equipo es original o no.

- **Switch:** Los Switch presentan la facilidad de realizar la conexión con las redes del Club Militar dentro de la Entidad y fuera de ella. Es importante la utilización de él porque permite la segmentación del tráfico de red, ocasionando mejoras en la velocidad de la misma

- **TCP/IP:** Es un conjunto de protocolos de red que implementa la pila de protocolos en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

- **Telnet:** Es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella.

- **TFTP:** Son las siglas de Trivial File Transfer Protocol (Protocolo de transferencia de archivos trivial).Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza

para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arrancan desde un servidor de red.

- **Trabajo Remoto (Teletrabajo):** Toda forma de trabajo que no requiera la presencia de la persona en la oficina o planta de la empresa. Para su realización deben actuar elementos telemáticos, ya sea computadoras, teléfonos o cualquier otra tecnología de la información y la Comunicación.

- **Troyano:** Es una pieza de software dañino disfrazado de software legítimo. Los caballos de troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño.

- **Ultrasecreto:** Tipo de clasificación de Información pertinente a actividades o planes de la defensa nacional interna o externa y a operaciones de inteligencia relativas a la misma, cuya divulgación no autorizada podría conducir a un rompimiento diplomático que afecte los interese de la nación a un ataque armado contra la misma o a destruir su estabilidad interna.

- **URL - Uniform Resource Locator:** El URL es un localizador uniforme de recurso. Es la cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en Internet. Existe un URL único para cada página de cada uno de los documentos de la World Wide Web, para todos los elementos del Gopher y todos los grupos de debate USENET, y así sucesivamente. El URL de un recurso de información es su dirección en Internet, la que permite que el navegador la encuentre y la muestre de forma adecuada. Por ello el URL combina el nombre del ordenador que proporciona la información, el directorio donde se encuentra, el nombre del fichero y el protocolo a usar para recuperar los datos. Y reemplaza la dirección numérica o IP de los servidores. Haciendo de esta manera más fácil la navegación, si no de otra forma se tendría que hacer bajo direcciones del tipo http://148.210.01.7 en vez de http://www.pagina.com.

- **Username (nombre de usuario):** Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un sistema.

- **Virus:** Es un programa que se copia automáticamente y que tiene por objeto alterar el funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

- **VLAN - Virtual Local Area Network:** Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares.

- **Vulnerabilidad:** Debilidad de un sistema que puede ser utilizada para violar las políticas de seguridad.

- **Wan -Wide Area Network:** Red de área extensa. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Véase también LAN y MAN.

- **WAP:** Wireless Application Protocol o WAP (protocolo de aplicaciones inalámbricas) es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, p.ej. acceso a servicios de Internet desde un teléfono móvil.

- **XML:** Es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Es una simplificación y adaptación del SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML).

- **Zona Desmilitarizada, Red Perimétrica (DMZ):** Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar.

6. NORMATIVIDAD

Se mencionan algunas de los marcos legales que, con un sistema de gestión de la seguridad de la información, debidamente implementado, se podrían cumplir en algunos de sus apartados:

LEY 527 DE 1999 que trata sobre Comercio Electrónico, 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 que trata sobre el delito Informático, de la protección de la información y de los datos.

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado o 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. [1]

LEY 1266 DE 2008 Habeas Data, la presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial de servicios y la proveniente de terceros países.

ARTICULO 15: Acceso a la información por parte de los usuarios.

La información contenida en Bancos de Datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países podrán ser accedidas por los usuarios únicamente con las siguientes finalidades:

Como elemento de análisis para establecer y mantener una relación contractual, cualquiera que sea su naturaleza, así como para la evaluación de los riesgos derivados de una relación contractual vigente.

Como elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas.

Para el adelantamiento de cualquier trámite ante una autoridad pública o una persona privada, respecto del cual dicha información resulte pertinente.

Para cualquier otra finalidad, diferente de las anteriores, respecto de la cual y en forma general o para cada caso particular se haya obtenido autorización por parte del titular de la información.

ARTICULO 20: Régimen de transición para las Entidades de Control.

La Superintendencia de Industria y Comercio y la Superintendencia Financiera asumirán, seis (6) meses después de la entrada en vigencia de la presente ley, las funciones aquí establecidas. Para tales efectos, dentro de dicho término el Gobierno Nacional adoptará las medidas necesarias para adecuar la estructura de la Superintendencia de Industria, Comercio y Financiera dotándola de la capacidad presupuestal y técnica necesaria para cumplir con dichas funciones.

CIRCULAR EXTERNA 052 de 2007 de la Superintendencia Financiera de Colombia que establece los requerimientos mínimos de seguridad y calidad que deben atender para el manejo de la información a través de los diferentes medios y canales utilizados para la distribución de los productos y servicios que ofrecen a sus clientes y usuarios, las entidades deberán tener en cuenta los criterios de seguridad de la información, confidencialidad, integridad y disponibilidad y los criterios de calidad de la información como la efectividad, la eficiencia y la confidencialidad.

LEY 489 DE 1998, diciembre 29. Sistema general de información administrativa del sector público.

ARTICULO 36. SISTEMA GENERAL DE INFORMACIÓN ADMINISTRATIVA. Créase el Sistema General de Información Administrativa del Sector Público, integrado, entre otros, por los subsistemas de organización institucional, de gestión de recursos humanos, materiales y físicos, y el de desarrollo administrativo. El diseño, dirección e implementación del Sistema será responsabilidad del Departamento Administrativo de la Función Pública en coordinación con los organismos competentes en sistemas de información, y de los cuales se levantará una memoria institucional.

ARTICULO 37. SISTEMA DE INFORMACIÓN DE LAS ENTIDADES Y ORGANISMOS.

Los sistemas de información de los organismos y entidades de la Administración Pública servirán de soporte al cumplimiento de su misión, objetivos y funciones, darán cuenta del desempeño institucional y facilitarán la evaluación de la gestión pública a su interior, así como, a la ciudadanía en general.

Corresponde a los comités de desarrollo administrativo de que trata la presente ley hacer evaluaciones periódicas del estado de los sistemas de información en cada sector administrativo y propender por su simplificación en los términos previstos en las disposiciones legales.

En la política de desarrollo administrativo deberá darse prioridad al diseño, implementación, seguimiento y evaluación de los sistemas de información y a la elaboración de los indicadores de administración pública que sirvan de soporte a los mismos.

LEY 603 DE 2000 Control de legalidad de Software, facultad a la Entidad para realizar verificaciones y enfatiza en la obligación de declarar en los informes de gestión el cumplimiento de las normas que protegen el software.

Y entre otras,

- Constitución Política de Colombia 1991.
- Ley 80 de 1993 “Estatuto General de contratación de la administración Pública”.
- Ley 87 de 1993 “Control interno en los organismos del Estado”.
- Ley 527 de 1999 “Comercio Electrónico”.
- Ley 594 del 2000 “Ley General de Archivo”.
- Ley 599 del 2000 “Código Penal Colombiano”.
- Ley 603 del 2000 “Control de legalidad del Software”.
- Ley 734 de 2002 “Código Disciplinario Único”.
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la Información”.
- Ley 1273 de 2009 “Protección de la Información y de los datos”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.
- Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
- Norma Técnica Colombiana NTC-ISO/IEC 27000
- Directiva No 2014-18 “POLITICAS DE SEGURIDAD DE LA INFORMACIÒN” de Min defensa.
- MINTIC: La aplicación de las 21 guías de seguridad y privacidad de la información MiPymes para implementar el sistema de seguridad de la información.

7. NIVELES DE AUTORIDAD Y RESPONSABILIDAD DE LA POLÍTICA

7.1 MISIONES PARTICULARES – ROLES Y RESPONSABILIDADES

7.1.1 ALTA DIRECCIÓN

Aprueba el Manual con las Políticas de Seguridad de la Información, de tal forma que muestra su apoyo, compromiso y motivación en el desarrollo, diseño e implementación de esta Política eficaz y efectiva la cual coadyuva en los lineamientos de la Entidad.

Así mismo este compromiso por parte de la alta Dirección se evidencia en:

- Revisión y aprobación de esta Política.
- Socialización a los funcionarios de la Política.
- Promover a través de campañas de sensibilización y concientización la Importancia de la Seguridad de la Información.
- Fortalecimiento de los recursos a fin de implementar y mantener las políticas establecidas.
- Verificación del Cumplimiento de la Política.

7.2 RESPONSABLE SEGURIDAD DE LA INFORMACIÓN

a) Definir y establecer las políticas de seguridad de la información, alineadas con las emitidas por el Ministerio de Defensa Nacional.

b) Coordinar la implementación de las políticas de Seguridad de la Información con los diferentes procesos de la Entidad.

c) Reportar a la Coordinación de Tecnologías de la Información el estado de la Seguridad de la Información del Club Militar.

d) Definir e implementar la estrategia de divulgación y concientización de Seguridad de la Información para todos los funcionarios y terceros que tengan acceso a los activos de información del Club Militar.

e) Evaluar, seleccionar y sugerir la implantación de herramientas que faciliten la labor de seguridad de la información.

f) Coordinar y ejercer control en el cumplimiento de las Políticas de Seguridad de la Información.

g) Recolectar los reportes de incidentes de seguridad de la información al correo seguridaddigital@clubmilitar.gov.co.

7.3 GRUPO GESTIÓN TIC

El Grupo Gestión TIC, debe realizar el proceso de asignación de usuarios, roles, permisos y responsabilidades de las herramientas tecnológicas que tenga la Entidad a los funcionarios que así lo requieran. Así mismo velar y promover el uso adecuado de la información, activos y herramientas informáticas con el fin de generar conciencia y garantizar la confidencialidad, integridad y disponibilidad de la información.

7.4 FUNCIONARIOS Y USUARIOS DE LOS SISTEMAS DE INFORMACIÒN

Los funcionarios (planta, personal en comisión, pasantes, prestación de servicios, outsorsing) deben clasificar los activos de información que se encuentren bajo su responsabilidad teniendo en cuenta la confidencialidad, integridad y disponibilidad de esta; así mismo verificar que se proporcione un nivel de protección de acuerdo a los lineamientos de la Política de Seguridad de la Información, y cumplir con:

- Promover el cumplimiento de la Política del personal que se encuentre bajo su responsabilidad.
- Implementar, monitorear y gestionar las herramientas tecnológicas para el cumplimiento de la Política de Seguridad de la Información.
- Implementar y administrar los controles necesarios para garantizar la seguridad de la información.
- Implementar estrategias de sensibilización y concientización a los funcionarios y terceros de la importancia de esta Política.
- Establecer, documentar, validar y actualizar los procedimientos de seguridad de la información que apliquen para las herramientas tecnológicas administradas por cada Grupo de Gestión.

7.5 GRUPO DE GESTIÓN TALENTO HUMANO

El Grupo de Gestión Talento Humano debe incluir en el proceso de inducción a los funcionarios internos como externos (planta, personal en comisión, pasantes, prestación de servicios entre otros) los temas de Seguridad de la Información donde se les informe del uso, responsabilidades e implicaciones en el manejo de los activos informáticos, así como la información contenida en ella.

7.6 OFICINA DE CONTROL INTERNO

Realizar las auditorías necesarias para verificar el cumplimiento y ejecución de la Política de Seguridad de la Información.

7.7 COORDINADORES DE GRUPO

El personal responsable de cada Grupo de Gestión debe velar por la confidencialidad, integridad y disponibilidad de los procedimientos que allí se manejen y brindarle la adecuada protección de acuerdo a las políticas establecidas.

7.8 GRUPO DE GESTIÓN ÁREA ADMINISTRATIVA

Esta dependencia tiene dentro de sus funciones realizar la revisión de requisitos para proceder a la posesión de un servidor público, trabajador oficial u prestadores del servicio. Como parte de la función de selección se debe realizar una verificación de los antecedentes (estudio de seguridad) y referencias de los candidatos, garantizar que los funcionarios firmen el acuerdo de confidencialidad.

7.9 OFICINA ASESORA JURÍDICA

Esta oficina es la responsable de garantizar que se incluyan las cláusulas de confidencialidad de la información dentro de los contratos de los contratistas.

8. CRITERIOS DE APLICACIÓN

8.1 SEGURIDAD EN LA ORGANIZACIÓN

Para garantizar los procesos en el Club Militar se tendrá en cuenta los siete fundamentos modelo en la seguridad de la información como son confidencialidad, integridad, disponibilidad, autenticidad, autorización, no repudio y auditabilidad.

Así mismo se debe contar con personal idóneo el cual tiene que estar en la capacidad de aprender, coordinar, asesorar, revisar, mantener, obtener y difundir todo lo relacionado con temas de seguridad; además se determina responsabilidades con el fin de tener claridad en la ejecución de tareas. Se debe tener certeza con el proceso de autorización a los servicios informáticos (software – hardware).

Siempre hay que tener un contacto directo con otras entidades, organizaciones y autoridades en caso de presentarse algún incidente informático con el fin de tener cooperación y lineamientos legales para su gestión.

Se debe tener claridad en todo lo relacionado con la revisión y realización de pruebas de vulnerabilidad con el fin de contar con un enfoque adecuado en la mitigación de los riesgos.

En lo referente al acceso a la información y activos informáticos a terceros siempre se debe tener el control, identificar posibles riesgos a nivel físico como lógico, cumplir con los requerimientos estipulados por el Grupo Gestión de Sistemas, informar sobre las responsabilidades, obligaciones, restricciones, procedimientos que puede llevar a cabo en las instalaciones.

Las políticas de seguridad de la información, tienen como objetivo garantizar el uso racional de los servicios informáticos, de internet, redes sociales y correo institucional, que se prestan en el Club Militar y en ningún momento pretenden ser una enunciación taxativa de la conducta y actos prohibidos toda vez que los actos que violan la constitución política la ley y demás normas y reglamentaciones nacionales como internacionales aceptadas en la comunidad de internet estén o no contempladas en la presente resolución están igualmente prohibidas.

Que el servicio de internet, redes sociales, correo institucional y demás sistemas de mensajería instantánea que la entidad disponga para el uso de los servidores públicos y contratistas deberán ser usados únicamente para las funciones asignadas a cada funcionario y para las actividades contratadas en caso de los contratistas.

Los funcionarios deben abstenerse de utilizar este medio para actividades de índole personal y para la participación en foros y comunidades en las que actúen a título personal y no como servidores públicos en caso de que se requiera la participación en nombre de la entidad sólo se podrá usar el correo institucional siempre y cuando exista una autorización del coordinador del grupo o jefe de oficina.

En el entendido que los equipos y servicios informáticos son herramientas de trabajo suministradas a los funcionarios y a los contratistas para el cumplimiento de sus labores, el contenido de los correos electrónicos es de propiedad e interés del Club Militar, susceptible de ser revisado en razón a su carácter no privado sino institucional u oficial; por lo tanto, la entidad se reserva el derecho de acceder a los correos institucionales, equipos y demás medios informáticos para verificar su correcto uso y puede utilizar la información encontrada

acuerdo las necesidades de la entidad y/o suministrarla a entes de control que la requieran dentro del marco de cualquier tipo de investigación.

Todos los funcionarios y contratistas del Club Militar deben conocer y aceptar estas condiciones de uso de los sistemas y equipos informáticos, previa a la asignación por parte de la entidad.

Que los usuarios del Club Militar que usen los servidores de internet y correo institucional y otros servicios informáticos deben mantener las normas de respeto, cortesía y responsabilidad, acorde a los derechos de los demás usuarios de internet que hagan usos de los servidores.

Se deben aplicar los siguientes procedimientos:

Para la creación de las cuentas de usuario, usuario de red, de cuentas de correo electrónico, de aplicaciones; se asignarán de manera individual a cada servidor público y se realizará mediante el registro de calidad denominado "SOLICITUD ACCESO A SERVICIOS INFORMATICOS", Código GT-M01-F04 y el GT-M01-F01 COMPROMISO DE CONFIDENCIALIDAD Y USO DE LA INFORMACION Obsoleto que se encuentra en la carpeta compartida de calidad de cada equipo unidad Y:/. El cuál debe ser diligenciado en su totalidad y estar revisado por el jefe inmediato, autorizado por el Profesional de Apoyo de la Oficina de Planeación y por la Dirección General; adjuntando la aceptación de las políticas de uso (PUA) con nombres, apellidos completos, número de identificación y huella.

El Club Militar, se reserva el derecho de asignar los nombres de las cuentas de usuario y la descripción, de acuerdo a las políticas de administración de correo institucional. Para las personas naturales vinculadas mediante contrato de prestación de servicios, convenio con un tercero ò convenios educativos, se deberá indicar en la descripción el nombre de la entidad contratista y diligenciar el formato denominado "COMPROMISO DE CONFIDENCIALIDAD Y USO DE LA INFORMACIÒN", para ser diferenciadas de los funcionarios. Los servidores públicos deben abstenerse de utilizar versiones escaneadas de firmas hechas a mano, para enviar correos o cualquier otro tipo de comunicación electrónica, en su nombre o de otra persona.

Para el uso de la Intranet e Internet de la Entidad, existen dos mecanismos de conexión: Alámbrica e inalámbrica (WI-FI), para los cuales el equipo debe estar debidamente identificado; para el caso de la conexión alámbrica a la Red LAN de la Entidad, debe estar autenticando contra el controlador de dominio del Club Militar, con usuario registrado y autorizado mediante formato de "SOLICITUD ACCESO A SERVICIOS INFORMATICOS", Código GT-M01-F04. Y se llevará a cabo en el marco de las políticas de uso de Internet y en las definidas por el sistema de Seguridad perimetral de la Entidad "FIREWALL". La navegación en sitios no seguros de Internet, tales como sitios de descarga de música, videos, sitios para adultos, redes sociales, los archivos ejecutables entre otros y que atenten contra la seguridad de la red está prohibida. En caso de requerirse por el cumplimiento propio de las funciones el acceso determinado a ciertas páginas como YouTube, Facebook, Twitter, entre otros debe presentarse solicitud en forma escrita al Comité de Seguridad de la Información indicando los links de las rutas y justificando su uso.

La Información consultada en cualquier horario de trabajo a través de Internet e Intranet, debe apoyar directamente las funciones relacionadas con el campo de responsabilidad laboral del servidor público y/o servir como herramienta para desempeñar sus funciones.

Las políticas y estándares documentan formalmente las reglas para la protección de la información del Club Militar, cuando se utilicen los servicios de Internet e Intranet y establecen que la información de la entidad debe ser protegida por todos los servidores públicos del Club Militar.

El Club Militar dispondrá de un sistema de firewall y antivirus que garantiza la defensa ante amenazas y posibles intrusiones a nivel externo y propagación de código malicioso a nivel interno, que afecte el desempeño de los recursos informáticos con que cuenta la entidad. Es responsabilidad de los usuarios informar oportunamente acerca de una sospecha de información por un virus, recepción de spam (mensajes no solicitados), o comportamiento anómalo por causas desconocidas, a la mesa de ayuda del Grupo Gestión TIC; ante estas situaciones de riesgo, deberá abstenerse de usar su computador y desconectarlo físicamente de la red. De igual manera es responsabilidad del funcionario informar sobre correos catalogados como extraños, fuera de contexto, extorsivos, anónimos que atenten contra la Entidad o la seguridad de la Información.

8.2 GESTIÓN DE ACTIVOS DE INFORMACIÓN

En lo referente a los activos fijos se debe tener en cuenta que cada usuario debe firmar un Acta de Novedad de activos fijos, responsabilidad y custodia sobre los activos informáticos que tendrá a cargo.

Se debe hacer referencia a la clasificación asignada a la información dependiendo el grado confidencial, restringida, reservada entre otros.

Se debe mantener un control efectivo sobre el software y hardware que la entidad posee para ello se cuenta con el área de activos fijos quien tiene el proceso y función para realizar esta labor.

Efectuar análisis de riesgos para obtener controles sobre las posibles amenazas.

8.3 GESTIÓN DE RECURSO HUMANO

En esta área se pretende determinar las responsabilidades, requisitos, obligaciones, deberes, derechos en lo relacionado con el uso de los activos informáticos, políticas de seguridad y normatividad que se deben tener con el personal que labora en la entidad, desde el momento que ingresa hasta el momento en que termina su relación laboral.

8.4 GESTIÓN, CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

Documento relacionado: **GLA-M04 MANUAL PARA LA CLASIFICACION DE INFORMACION Y DATOS PERSONALES**

Se considera información a toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere el Club Militar, como, por ejemplo: Formularios / comprobantes propios o de terceros. Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel. Otros soportes magnéticos/electrónicos removibles, móviles o fijos. Información transmitida vía oral o por cualquier otro medio de comunicación.

Toda la información deberá ser identificada, clasificada y documentada. Los usuarios responsables de la información del Club Militar, deben identificar los riesgos a los que está expuesta la información de sus áreas,

teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Los niveles de clasificación de la información que se han establecido de acuerdo a los contenidos de los Datos son:

- Datos sensibles.
- Datos privados.
- Datos Semiprivados y Datos Públicos.

El Club Militar determinará los niveles a requerir para clasificar la información de acuerdo con su sensibilidad, posterior se debe realizar una guía de Clasificación de la Información para que los propietarios (Coordinadores de Grupos de Gestión y el área de Gestión Documental) de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda información generada por el Club Militar debe ser identificada, clasificada y documentada de acuerdo a la guía de Clasificación de la Información, así mismo se requiere recursos para aplicar los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información, todo esto se realiza a fin de promover la importancia, cultura de uso de la seguridad de la información a los funcionarios internos y externos de la Entidad.

Se tiene en cuenta y aplica la Guía No. 5 para la Gestión y Clasificación de Activos de Información de MINTIC, debidamente clasificada en el respectivo índice información reservada clasificada del Club Militar, teniendo en cuenta los criterios de clasificación.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1: Criterios de Clasificación

Fuente: Guía No. 5 MINTIC

La seguridad del Entorno brinda las medidas de seguridad perimetral que se deben tener en todos aquellos sitios en los cuales se encuentren equipos y activos informáticos de la Entidad, adicional en los centros de cómputo de las tres sedes en los cuáles debe existir un control de acceso restringido y solo acceda personal autorizado, contar con sistemas de control y detección de incendios, detección de intrusos, registro de ingreso y salida,

clasificación del tipo de información, aplicación de normas de seguridad industrial, planes de emergencia en caso de un incidente.

A nivel de equipos estos deben contar con pólizas de seguros, con el fin de prevenir robos, incendio, explosión o cualquier otra eventualidad.

Se debe contar con sistemas de contingencia como lo es SUMINISTRO DE ENERGÍA SIN INTERRUPCIÓN (UPS).

Contar con el mantenimiento tanto preventivo como correctivo de la parte eléctrica, equipos activos, cableado estructurado con el fin de mantener en óptimas condiciones dichos elementos.

Se debe contar con un proceso determinado en el momento en que un activo informático salga de las instalaciones de la Entidad, toda vez que puede ser objeto de pérdida, robo y con ello se evidencia una vulnerabilidad con la información contenida en el mismo.

8.5 GESTIÓN CONTROL DE ACCESO

El control de acceso hace referencia a las políticas que se deben tener en cuenta para el acceso de los usuarios a los datos, red, información entre otros.

A nivel de usuario este debe tener un ID (identificador) que lo identifique como único dentro de la red, al cual se les darán permisos a los diferentes sistemas de información, correo electrónico, acceso remoto, acceso web.

Se debe determinar el tipo de perfil de usuario dependiendo la información a acceder, el grado de clasificación, el cargo que ocupa y el tiempo de permanencia en la Entidad.

Cuando un usuario cambie de cargo o se retire de la entidad debe informar de forma inmediata con el fin de restringir los privilegios a los diferentes sistemas de información.

El administrador del sistema o funcionario encargado debe contar con un registro de creación, modificación, eliminación de todos los usuarios, perfiles, privilegios y accesos que tengan en la entidad.

Se crea una política para que la contraseña sea cambiada al inicio de sesión cuando es por primera vez, y de forma mensual o cada vez que el usuario requiera su cambio, debe ser diferente a las últimas dos contraseñas descritas, debe tener un mínimo de caracteres establecido, debe ser única e intransferible, se debe informar al usuario que el uso y manipulación de la misma es responsabilidad del mismo y cualquier inconveniente presentado será objeto de verificación de acuerdo a las normas establecidas.

Los administradores o funcionarios encargados del sistema deben estar en constante verificación de las aplicaciones, efectuar copias de respaldo, auditorías y velar por el mantenimiento de los equipos, depurar los usuarios existentes, verificar perfiles, accesos y monitorear de forma constante los equipos y la red de posibles vulnerabilidades, ataques de códigos maliciosos o malintencionados.

Para todo equipo o software que se instale en la Entidad se debe cambiar el usuario o contraseña por defecto (default).

Se debe tener especial cuidado con aquellos equipos que se encuentren fuera de uso o desatendidos con el fin de verificar si existe o no información sensible en ellos, generar un backup, realizar un diagnóstico; determinar si estos equipos se pueden utilizar en otras dependencias de lo contrario realizar el concepto técnico y proceder a dar de baja por intermedio del área de activos fijos.

Los equipos deben contar con política de bloqueo de sesión en un determinado tiempo, deben contar con antivirus actualizado y software de seguridad (antispam- anti keylogger, firewall personal).

Se debe mantener un control en lo referente a los horarios de acceso a los sistemas de información teniendo en cuenta el tipo de usuario, cargo, responsabilidad.

El acceso a la red del Club Militar está determinado por procedimientos claros y solo se acceda a lo autorizado, se prohíbe todo aquello que afecte los intereses de la entidad teniendo en cuenta que los equipos son para uso institucional y no comercial ni personal.

En lo que tiene que ver con las conexiones a redes inalámbricas éstas deben encontrarse separadas de los servicios y sistemas de información, protegidos por perímetros de seguridad establecidos.

Se debe tener control en el acceso hacia las conexiones de redes, controles de enrutamiento, validar fuentes en las puertas de enlace (Gateway), control sobre las redes compartidas, tiempos de desconexión (tiempo muerto).

Siempre debe existir un monitoreo y gestión de todos los servicios y sistemas de información, llevar registros, análisis de vulnerabilidades, posibles infiltraciones, mantenimientos preventivos y correctivos, registros de eventos.

Cuando se utilice por cualquier razón equipos personales en las labores cotidianas se debe tener cuidado en el tipo de información que se almacene en estos equipos.

Cuando por algún motivo o circunstancia un equipo de la entidad se pierde o es hurtado el usuario debe tener conocimiento de los requisitos legales, seguros y responsabilidad del mismo.

8.6 GESTIÓN COMUNICACIONES

Para que exista un entorno funcional se debe trabajar en conjunto la parte de infraestructura tecnológica y de controles de seguridad para garantizar la disponibilidad, integridad y confidencialidad de la información.

El Club Militar establecerá criterios para nuevos sistemas de información, se llevará a cabo pruebas necesarias para adecuar el sistema, se evaluará la aplicabilidad y se dará el aval para su aceptación y puesta en funcionamiento, y actualización de los existentes para contribuir en la mejora y funcionabilidad.

El Club Militar debe implementar controles para la prevención, detección y recuperación de ataques pasivos o activos tanto de la parte física como lógica, así como procedimientos apropiados para su instalación, configuración y administración.

Se debe contar con copias de respaldo con el fin de realizar actividades de restauración de los diferentes sistemas con que se cuenta en la actualidad, estas se harán desde las copias del software original.

Los activos informáticos (software y hardware) deben contar con cuentas, usuarios, contraseñas, accesos o autorizaciones supervisadas por el Grupo Gestión de sistemas y no se recomienda dejar instalaciones por defecto o de fábrica toda vez que es un foco de vulnerabilidad.

8.7 GESTIÓN DESARROLLO Y MANTENIMIENTO SISTEMAS DE INFORMACIÓN

El Club Militar debe disponer de procedimientos para garantizar la seguridad y calidad de los sistemas e información desarrollada para determinadas tareas en la entidad.

Todo software que sea utilizado con fines misionales debe contar con manuales de instalación, manuales de usuario, manual técnico, código fuente, ciclo de vida, y su correspondiente soporte, esto acorde con los lineamientos de la Entidad.

Para garantizar el correcto funcionamiento de los activos informáticos se debe realizar contratos de mantenimiento los cuales estarán bajo la supervisión permanente de un funcionario del Grupo de Gestión de Sistemas el cual estará encargado de supervisar, controlar y verificar que se cumplan los lineamientos previamente solicitados para tal fin.

8.8 GESTIÓN DE CONTINUIDAD DE NEGOCIO

El Club Militar debe proporcionar los recursos suficientes a fin de generar una respuesta oportuna en caso de presentarse una contingencia o evento que afecte la continuidad del Negocio, teniendo en cuenta que debe responder de forma efectiva ante este tipo de eventualidades según su magnitud y grado de afectación, así mismo se deben restablecer los servicios y operaciones minimizando costos y posibles pérdidas, protegiendo la seguridad de la información durante la ejecución de estos eventos.

En cumplimiento con la guía 9 de MINTIC para la preparación de las TIC para la continuidad del negocio del Club Militar elaboro el plan de continuidad del negocio CM-FT-PL_01 Versión 2.

8.9 GESTIÓN DE RIESGOS

En la aplicación de la guía 7 de seguridad y privacidad de la información en cuanto a gestión de riesgos, la Entidad identifico los siguientes riesgos:

Item	Identificación del riesgo					
	Riesgo	Activos	Tipo	Vulnerabilidad	Clasificación del Riesgo	Frecuencia actividad
1	a. Perdida de la Disponibilidad	Sistemas de Informaciòn e Infraestructura TIC`s	f. Organización	Ausencia de planes de continuidad	d. Tecnología	365
2	c. Perdida de la Integridad	Informaciòn digital alojada en sistemas de informaciòn del Cm	f. Organización	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	d. Tecnología	365
3	b. Perdida de la Confidencialidad	En la configuraciòbn de seguridad de los sistemas de información e infraestructura TIC`s del CM.	f. Organización	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	d. Tecnología	365

Identificación del riesgo							Identificación del riesgo							Identificación del riesgo							Identificación del riesgo					
Riesgo	Activos	Tipo	Vulnerabilidad	Clasificación del Riesgo	Frecuencia actividad	Item	Riesgo	Activos	Tipo	Vulnerabilidad	Clasificación del Riesgo	Frecuencia actividad	Item	Riesgo	Activos	Tipo	Vulnerabilidad	Clasificación del Riesgo	Frecuencia actividad	Item	Impacto	Proceso, procedimiento o actividades sucetibles.	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia actividad
a. Perdida de la Disponibilidad	de los registros documentales en custodia de los archivos fisicos.	e. Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.	d. Tecnología	365	5	c. Perdida de la Integridad	de los registros documentales generados en cada una de las areas organizacionales del CM.	f. Organización	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	d. Tecnología	365	6	c. Perdida de la Integridad	de los registros documentales generados en cada una de las areas organizacionales del CM.	f. Organización	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	d. Tecnología	365	7	c. Economico y Reputacional		Posibilidad de alteración, interrupción o manipulación de las configuración o datos contenidos en los sistemas de información con el fin de favorecer intereses particulares o internos de la entidad.	c. Corrupción	e. No se ha presentado en los últimos 5 años

8.10 REQUERIMIENTO LEGALES

Aquí se hace referencia a las disposiciones, perjuicios, responsabilidades, autorizaciones, efectos legales que se deben tener en cuenta en el manejo de la información que posee la Entidad y que los usuarios deben acatar con el principio de la confidencialidad dependiendo el cargo y funciones asignadas, toda vez que el “desconocimiento de la norma no lo exime de la responsabilidad”.

El Club Militar debe crear requerimientos de seguridad para que los usuarios, contratistas, personal externo cumplan bajo las normas y estándares legales establecidos para el uso, adquisición, desarrollo e implementación de activos informáticos

8.11 CUMPLIMIENTO

Todos los usuarios de los activos informáticos del Club Militar, responsables por acción u omisión del incumplimiento de las políticas de seguridad informática o violación de los estándares de seguridad informática, estarán sujetos a las sanciones administrativas, disciplinarias o penales a que haya lugar, de acuerdo con lo establecido en la legislación colombiana, sin perjuicio de la responsabilidad civil por las consecuencias que de estas acciones u omisiones se deriven.

Esta Oficina se encargará de identificar, documentar y mantener los requisitos legales aplicables a la Entidad en referencia a la Seguridad de la Información.

El Grupo Gestión TIC debe velar y garantizar que todo el software de la Entidad esté protegido por Derechos de Autor, así mismo su licencia de uso o software libre de distribución y uso.

Así mismo se debe establecer un inventario de software y sistemas de información de todos los equipos de la Entidad, verificar que lo instalado sea lo permitido, e informar a los usuarios la no instalación de software sin previa autorización del Grupo Gestión de Sistemas.

Los usuarios o funcionarios de la Entidad deben conocer, entender y cumplir con la Ley de Derechos de Autor y licenciamiento de software, teniendo en cuenta que la reproducción no autorizada es una violación de la ley.

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales el Club a través de la Oficina Jurídica, Control Interno contribuirá por la Protección de los Datos de los Socios, familias, terceros entre otros, de los cuales se reciba y administre información, por tanto, la Entidad hará el uso adecuado de esta información brindando la protección y privacidad adecuada a los mismos.

Esta protección y privacidad de información también se debe realizar a los funcionarios que laboran en la Entidad, a través de controles que preserven la integridad, disponibilidad y confidencialidad de los datos haciendo un uso solo en las funciones propias de la Entidad, sin ser publicadas, reveladas o entregadas sin previa autorización.

8.12 POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Las políticas específicas están definidas para el club Militar, sobre los siguientes aspectos:

8.13 EN LA GESTIÓN DE TERCEROS

Cuando exista la necesidad de otorgar acceso de terceras partes al CLUB MILITAR, deberá realizarse siempre con la participación del propietario de la información, una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre los siguientes aspectos:

- El tipo de acceso requerido (Físico, lógico y a que recurso).
- Los motivos para los cuales solicita el acceso.
- El valor de la información.

Los controles empleados por la tercera parte.

a) En todos los contratos cuyo objeto sea la prestación de servicios a título personal, bajo cualquier modalidad jurídica, que deban desarrollarse dentro de las instalaciones del CLUB MILITAR, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.

b) En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicio críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

c) El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo. Este, junto con la oficina de Informática, aprobará y autorizaran el acceso y uso de la información.

d) Los contratos o acuerdo de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores deben contemplar los requisitos legales aplicables.

8.14 EN LOS ACUERDOS DE CONFIDENCIALIDAD

Todos los empleados públicos y terceros deben firmar el compromiso de confidencialidad y uso de la información de confidencialidad que deberá ser parte integral de los contratos, utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de

información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas. FORMATO COMPROMISO DE CONFIDENCIALIDAD Y USO DE LA INFORMACIÒN.

8.15 EN ACUERDOS DE INTERCAMBIO DE INFORMACIÓN Y SOFTWARE

a) Todo empleado público y/o tercero es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

b) Los propietarios de información que se requiera intercambiar, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad de acuerdo a la documentación vigente.

c) El intercambio de información y de software con otras entidades, se realiza previa celebración de convenio interadministrativo en el que se establecen cláusulas de responsabilidad, deberes y derechos.

d) Los acuerdos de intercambio, deben en todo caso velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo deben especificar las consideraciones de seguridad y reserva de la información, y las responsabilidades por el mal uso o divulgación de la misma.

e) Cuando la información sea solicitada por autoridad judicial o administrativa competente; la entrega se realizará siguiendo el procedimiento establecido por la entidad que solicita la información.

f) El intercambio de información deberá contemplar las siguientes directrices:

- Uso de WebServices, para la publicación y consumo de información electrónica.
- Uso de canales cifrados.
- Respeto por los derechos de autor del software intercambiado.
- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido por el receptor de la información.
- Informar al titular de los datos, el intercambio de estos con otras entidades.
- Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

8.16 DEL USO DE INTERNET

a) El servicio de internet, redes sociales, correo institucional y demás sistemas de mensajería instantánea que la entidad disponga para el uso de los servidores públicos y contratistas deberán ser usados únicamente para las funciones asignadas a cada funcionario y para las actividades contratadas en caso de los contratistas.

b) Los funcionarios deben abstenerse de utilizar este medio para actividades de índole personal y para la participación en foros y comunidades en las que actúen a título personal y no como servidores públicos

en caso de que se requiera la participación en nombre de la entidad sólo se podrá usar el correo institucional siempre y cuando exista una autorización del coordinador del grupo o jefe de oficina.

c) En el entendido que los equipos y servicios informáticos son herramientas de trabajo suministradas a los funcionarios y a los contratistas para el cumplimiento de sus labores, el uso de internet será objeto de monitoreo permanente de tiempos de navegación y páginas visitadas por los empleados públicos y terceros autorizados. Así mismo, se pueden inspeccionar, registrar o informar las actividades realizadas durante la navegación.

d) Todos los funcionarios y contratistas del Club Militar deben conocer y aceptar estas condiciones de uso de Internet, previa autorización por parte de la entidad.

e) Los empleados del Club Militar que usen los servidores de internet y correo institucional y otros servicios informáticos, deben mantener las normas de respeto, cortesía y responsabilidad, acorde a los derechos de los demás usuarios de internet que hagan usos de los mismos.

En ningún caso se consideran aceptables los siguientes usos:

1. Navegación en sitio de contenido sexualmente explicito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
2. Publicación o envío de información confidencial hacia afuera del CLUB MILITAR sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
3. Utilización de otros servicios disponibles a través de internet que permitan establecer conexiones o intercambios no autorizados.
4. Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el jefe de la oficina.
5. Promover o mantener asuntos o negocios personales.
6. Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
7. Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la Entidad.
8. Uso de herramientas de mensajería instantánea no autorizadas por la oficina de informática.
9. Emplear cuentas de correo externas, no corporativas, para el envío o recepción de información institucional.

8.17 USO DE CORREO ELECTRÓNICO INSTITUCIONAL Y CORPORATIVO

POLÍTICAS DE USO: Sin perjuicio de las directrices que imparta la Coordinación del Grupo de Gestión TIC, los servidores públicos y demás prestadores de servicios bajo cualquier modalidad de contratación, deben cumplir con las políticas de administración publicación y uso de la información vía Intranet e Internet y los lineamientos de comportamiento apropiado que se definen en la presente resolución.

a) Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.

b) Las cuentas de correo institucional son de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente, y no prestarla bajo ninguna circunstancia.

c) El correo electrónico institucional es una herramienta de trabajo, de uso exclusivamente laboral e institucional, por lo que la información contenida en estos es de propiedad del Club Militar. Por lo tanto, el Club Militar se reserva el derecho de verificar, auditar, hacer trazabilidad, descargar la información contenida en los correos electrónicos institucionales y usar esta información como medida probatoria a nivel de investigaciones disciplinarias internas o externas y se reserva el derecho de entregarlas a los entes de control que así lo requieran.

d) Las cuentas de correo institucional son creadas para el uso exclusivo de actividades relacionadas con las funciones propias de cada cargo, por lo tanto, el usuario debe hacer uso de este servicio implementando criterios de racionalidad, respeto, responsabilidad, integridad y seguridad de la información.

e) Es responsabilidad del usuario realizar copias de seguridad o solicitar las copias de seguridad del archivo que almacena la información contenida en el correo y de la libreta de direcciones. Antes de enviar un correo electrónico, el usuario debe utilizar el corrector ortográfico de la herramienta que utilice como gestor del correo.

8.18 PROHIBICIONES

a) El envío de correos con mensajes que contravengan las normas legales, la moral, el orden público, la intimidad o el buen nombre de las personas, que contengan contenido irrespetuoso, difamatorio, racista, religioso, discriminatorio, de acoso o intimidación; así como imágenes o videos con contenidos ilegales, ofensivo, extorsivo, indecente o con material sexual.

b) Al ser el correo electrónico institucional la herramienta dispuesta por el Club Militar como medio de comunicación oficial, se prohíbe el uso de correos personales con el fin de transferir información institucional.

c) Está prohibido copiar o reenviar correos electrónicos que se encuentren clasificados como CLASIFICADOS o SECRETOS en el asunto del mensaje, sin tener la autorización del remitente original para hacerlo.

d) Usar el correo electrónico institucional para el envío de propaganda, ofertas, negocios personales, avisos publicitarios o cualquier información ajena a las laborales propias del cargo.

e) La propagación de correos de procedencia desconocida, SPAM, correo basura o no deseado, hacia cuentas institucionales.

f) Usar el correo electrónico como herramienta de mensajería instantánea.

g) Compartir contactos o listas de distribución de la Club Militar con personal externo, con el objetivo de propiciar el envío de propagandas, ofertas, negocios personales, avisos publicitarios, o información de otro tipo, ajena a las labores propias del cargo.

h) Usar el correo electrónico institucional del Club Militar debe ser usado únicamente para propósitos laborales.

i) Enviar mensajes ofensivos; injuriosos, cadenas de mensajes o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la Institución.

j) Utilizar una cuenta de correo electrónico que pertenezca a otra persona. En caso de ausencias o vacaciones, se debe recurrir a mecanismos alternos como re- direccionar los mensajes.

k) Las cadenas de mensajes de cualquier tipo y la propaganda de tipo comercial, político o religioso entre otros y, cualquier contenido ofensivo para los funcionarios de la Club Militar

8.19 ENVIO DE CORREOS MASIVOS: El área de Comunicaciones y Mercadeo del Club Militar es la autorizada para el envío de correos masivos y comunicados a los socios. En caso que alguna área, departamento o persona requiera enviar algún correo masivo, deberá solicitarlo al área de comunicaciones, quienes evaluarán la pertinencia o no de dicha solicitud. La cuenta autorizada para el envío de correos masivos institucionales es comunicaciones@clubmilitar.gov.co

8.20 NORMAS PARA UNIFICAR LOS CORREOS ELECTRONICOS Y FORTALECER LA IMAGEN INSTITUCIONAL DEL CLUB MILITAR

- Los correos electrónicos institucionales deben estar escritos en las fuentes Arial, tamaño 12.
- El texto debe estar escrito únicamente en color negro.
- No se debe escribir en mayúsculas. Ya que puede ser interpretado como un grito u ofensa.
- Los correos enviados no deben tener ningún color o imagen sobre el fondo en el que se escribe el mensaje.
- Se recomienda seguir las normas del Sistema de gestión de la calidad en el mismo formato de comunicados. Cartas o memorandos. Acceso directo de su Equipo icono Calidad unidad Y:/.

8.21 FIRMA DEL CORREO Y DISCLAIMER

Cada funcionario del Club Militar deberá tener una firma en el correo electrónico institucional. Las firmas se presentarán en el siguiente orden: nombre completo y apellidos; cargo, dependencia, nombre de la Institución, teléfono de contacto, dirección del Club Militar, correo electrónico y pagina Web www.clubmilitar.gov.co., logos del Club Militar y del proceso de acreditación de calidad institucional.

Ejemplo:

PEDRO JOSE PEREZ

Oficina XXXX

Club Militar

Teléfonos: 2 90 50 77 EXT 2309

Carrera 50 No. 15 - 80

CLUB MILITAR

APP: "Actitud, perseverancia y pasión"

pperez@clubmilitar.gov.co | www.clubmilitar.gov.co

Política Cero papel: "NO imprima este mensaje si no es necesario" en el Club Militar estamos comprometidos con la Protección y Cuidado del Medio Ambiente.

8.22 USO DE HERRAMIENTAS INALAMBRICAS

a) Se debe propender por la implementación de ambientes de trabajo completamente independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a la red Institucional.

b) Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta a identificación, autenticación, control de contenido de internet y cifrado entre otros.

c) Se debe implementar infraestructura inalámbrica que permita configuraciones de seguridad. En ningún caso se podrá dejar las configuraciones y contraseñas establecidas

8.23 EN SEGMENTACIÓN DE REDES

a) La plataforma tecnológica del CLUB MILITAR, que soporta los sistemas de información debe estar separada en segmentos de red físicos y lógicos VLANS, e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet.

b) La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos, de enrutamiento y de seguridad, si así se requiere. La oficina de Informática es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

8.24 COMPUTACIÓN EN LA NUBE (CLOUD COMPUTING)

a) Se podrá implementar servicios de nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

b) Se debe garantizar que por ningún motivo se almacene información clasificada en servicios en la nube públicos o híbridos.

8.25 DERECHOS DE PROPIEDAD INTELECTUAL

a) El Club Militar cumplirá con la reglamentación vigente sobre propiedad intelectual, para lo cual implementará los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

b) No se permitirá el almacenamiento, descarga de internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

c) Se permitirá el uso de documentos, cifras y/o textos de carácter público, siempre y cuando se cite el autor de los mismos, con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

d) Los procesos de adquisición de aplicaciones y paquetes de software, cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

e) El software ERP, a la medida, adquirido a terceras partes o desarrollado por funcionarios del CLUB MILITAR, serán de uso exclusivo de la Entidad y la propiedad intelectual será de quien lo desarrolle.

8.26 CONTROL DE CAMBIOS

a) Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la oficina de TIC, y debe cumplir con

una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

b) Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones, controles y deben ser definidos en un procedimiento de Control de Cambios.

8.27 CONTROL DE VERSIONES

a) Antes de la puesta en producción de una aplicación nueva, o de la actualización de las plataformas existentes, se debe asignar un número de edición o versión a la misma, y se debe contar con un procedimiento de Control de Versiones.

b) El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.

c) Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde solo se permita el acceso al personal autorizado.

d) Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son iguales.

8.28 SEPARACIÓN DE AMBIENTES

a) El Club Militar proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.

b) El paso de actualizaciones de software y hardware, de un ambiente a otro, deberá ser controlado y gestionado de acuerdo con lo definido en el procedimiento de Control de Cambios.

c) Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción, así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

d) No deberán realizarse pruebas, instalaciones, actualizaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.

e) El ambiente del sistema de prueba debe emular el ambiente de producción, lo más completo posible.

8.29 RECURSOS TECNÓLOGICOS

a) La instalación de cualquier tipo de software en los equipos de cómputo del CLUB MILITAR es responsabilidad exclusiva de la oficina de Informática, por tanto, son los únicos autorizados para realizar esta labor.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por la oficina TIC del Club Militar.

c) Los equipos de cómputo asignados, deben ser devueltos a la dependencia responsable, una vez sean reemplazados o cuando el funcionario o tercero responsable de dicho equipo finalice su vinculación con el CLUB MILITAR.

d) De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de cómputo en las oficinas, una vez se haya cesado el uso de los mismos.

8.30 CONCIENTIZACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

a) Se debe mantener un programa anual de concientización y capacitación para todos sus funcionarios, así como para los contratistas y terceros que interactúen con la información institucional y desarrollen actividades dentro de la Entidad.

b) Todos los funcionarios y terceros al servicio del CLUB MILITAR, deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

8.31 FINALIZACIÓN DE LA RELACIÓN LABORAL

Al momento de la desvinculación o de cambio de funciones, todo empleado y/o tercero debe hacer entrega de todos los activos de información que le hayan sido asignados. Esto mediante un formato establecido por el grupo TIC del Club Militar.

8.32 SEGURIDAD FÍSICA

a) Se consideran áreas de acceso restringido a todas las áreas donde se encuentran alojados los equipos como Servidores o almacenamiento de información privada, equipos de cómputo, la infraestructura de soporte a los sistemas de información y comunicaciones, y las áreas donde se encuentra la documentación privada del CLUB MILITAR; por lo cual se deben emplear mecanismos de acceso físico que garanticen que sólo se permite el acceso al personal autorizado.

b) El acceso a las áreas restringidas por parte del personal de soporte técnico d se debe otorgar y monitorear, únicamente cuando sea necesario por medio de una autorización.

c) Todas las puertas que utilicen sistema de control de acceso, deberán permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados, evitar que las puertas se dejen abiertas.

d) No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la Entidad, a menos que esté autorizado.

e) Los funcionarios y terceros, así como los visitantes, deberán tener acceso físico restringido a los sitios que requieran y les sean autorizados para el cumplimiento de sus funciones, tareas o misión dentro de las instalaciones del CLUB MILITAR.

f) Todos los escritorios o mesas de trabajo deben permanecer ordenados y asegurados con el fin de no exponer elementos con información crítica tales como documentos físicos y dispositivos de almacenamiento ante visitantes mal intencionados y de esta forma reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

8.33 SEGURIDAD Y MANTENIMIENTO DE EQUIPOS

a) Los equipos que hacen parte de la infraestructura tecnológica del CLUB MILITAR, deben ser ubicados y protegidos adecuadamente para prevenir la perdida, daño, robo o acceso no autorizado de los mismos.

b) Se adoptarán los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

c) Los funcionarios y terceros velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.

d) Los equipos portátiles deberán estar asegurados (cuando estén desatendidos) con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones del CLUB MILITAR.

e) Se debe garantizar la existencia de pólizas o seguros para la reposición de los activos informáticos que respaldan los planes de contingencia y la continuidad de los servicios.

8.34 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

a) Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones del CLUB MILITAR, deben velar por la protección de los mismos, sin dejarlos desatendidos, comprometiendo la imagen o información de la Entidad.

b) El propietario del activo, con el apoyo de la oficina de Informática, identificará mediante una tecnología de análisis de riesgos; las vulnerabilidades potenciales que puede generar el retiro de equipos o medios, de las instalaciones; así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.

c) En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información relacionada con la defensa y la seguridad nacional, se deberá realizar inmediatamente el respectivo reporte, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad, y se deberá poner la denuncia ante la autoridad competente, si aplica.

d) Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones del CLUB MILITAR, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o que puedan poner en riesgo la información que contiene.

8.35 TRASLADO FUERA DE ENTIDAD

a) El retiro de equipos o medios que procesan o almacenan algún tipo de información y/o que hacen parte de la plataforma tecnológica del CLUB MILITAR, debe ser autorizado por el propietario del activo, previa solicitud del funcionario interesado.

b) Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones del CLUB MILTAR, debe ser debidamente identificado y registrado antes de conceder la autorización respectiva.

8.36 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

a) Los sistemas operacionales y aplicaciones deberán actualizarse según lo definido en los procedimientos de Gestión de Vulnerabilidades Técnicas y Control de Cambios

b) Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información deberán estar protegidos mediante herramientas de software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.

c) Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la oficina de Informática; y deberán ser actualizados periódicamente.

d) No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación, diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

e) Todos los medios de almacenamiento que se conecten a equipos de la infraestructura tecnológica del CLUB MILITAR, deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

f) La oficina de Informática será responsable de que los usuarios del CLUB MILITAR mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

g) Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

8.37 COPIAS DE RESPALDO

a) Se debe asegurar que la información centralizada en el ERP de la Entidad y las dependencias responsables de la misma, contenida en la plataforma tecnológica del CLUB MILITAR, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, lo cual debe estar definido en el Procedimiento de Gestión de Backus y recuperación.

b) Los medios de las copias de respaldo se almacenarán tanto localmente como en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.

c) Se deberá establecer un plan de restauración de copias de seguridad que será probado de acuerdo al tipo de copia realizada incremental o full, establecidos según las necesidades del Club, con el fin de asegurar su adecuada restauración.

d) El Grupo de Gestión TIC, establecerá los procedimientos de backup y recuperación de la información que incluyan especificaciones acerca de su frecuencia y registro; así mismo, definirá conjuntamente con los grupos de gestión los periodos de realización de copias de usuario final

8.38 GESTIÓN DE MEDIOS REMOVIBLES

a) La conexión de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales, debe ser autorizada mediante formato.

b) Los medios de almacenamiento removibles como cintas, discos duros, CDs, DVDs, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, deben ser controlados y físicamente protegidos

c) El Grupo Gestión TIC, con debida autorización del subdirector del Club Militar, definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas en los sistemas de información y en la plataforma tecnológica, en caso de ser requerido para el cumplimiento de sus funciones.

d) Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene y debe tener un responsable asignado.

8.39 COMPUTACIÓN MÓVIL

a) Para el uso de dispositivos institucionales de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se debe implementar controles de acceso y técnicas criptográficas para cifrar la información crítica almacenada en estos.

b) La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser debidamente autorizada por el Grupo TIC, previa verificación de que cuenten con las condiciones de seguridad, estableciendo los mecanismos de control necesarios para proteger la infraestructura.

8.40 GESTIÓN DE RIESGOS – LOGS

a) Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento de red y de seguridad informática, deberán generar registros de eventos LOG, que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información

b) El tiempo de retención de los Logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen al Sector Defensa.

c) El lugar de retención de los registros estará definido por el nivel de clasificación de información que posean dichos registros.

d) Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado al Grupo Gestión TIC, y se debe establecer el procedimiento de Gestión de Incidentes y realizar su respectivo seguimiento.

8.41 CONTROL DE ACCESO

a) Los sistemas de información y dispositivos de procesamiento, seguridad informática y comunicaciones contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

b) Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad Informática del CLUB MILITAR, deberá estar autorizado por el Grupo Gestión TIC.

c) Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso, el tráfico de datos deberá estar cifrado.

d) La creación, modificación, y baja de usuarios en la infraestructura de procesamiento de información, comunicaciones y seguridad informática deberá seguir el formato y procedimiento de SOLICITUD ACCESO A SERVICIOS INFORMATICOS", Código GT-M01-F04.

e) La asignación de privilegios en las aplicaciones para los diferentes usuarios estará determinada por el procedimiento **SOLICITUD ACCESO A SERVICIOS INFORMATICOS", Código GT-M01-F04.** Estos privilegios deben revisarse a intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por traslados, cambios de cargo o terminación de la relación laboral.

8.42 SEGURIDAD DEL CENTRO DE DAOS Y CENTRO DE CABLEADO

a) No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos se debe registrar las personas que van a ingresar al software de control de acceso y se entregara una tarjeta para acceder a los controles biométricos para que su ingreso quede registrado y se pueda hacer seguimiento.

b) El grupo de Gestión TIC debe garantizar que el control de acceso al centro de datos del CLUB MILITAR, debe contar con dispositivos electrónicos de autenticación o sistema de control biométrico.

c) El Grupo TIC, deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.

d) La limpieza y aseo del centro de datos estará a cargo del Grupo Gestión TIC. Esta labor no será realizada por ninguna otra persona ajena a esta dependencia, con el fin de evitar alguna desconexión en los servicios.

e) En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

El centro de datos debe estar provisto de:

a) Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.

b) Pisos elaborados con materiales no combustibles.

c) Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.

d) Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.

e) Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

f) Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

g) El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.

h) Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

i) La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el Grupo Gestión TIC y exclusivamente con fines institucionales.

j) Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado del CLUB MILITAR.

k) Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.

l) Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

m) Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

n) Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

8.43 USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN

a) Los documentos que se impriman en las impresoras del CLUB MILITAR deben ser de carácter institucional, por ningún motivo se deben realizar impresiones u otro servicio de carácter personal.

b) Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

c) Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

8.44 USO DE UNIDADES DE RED Y CARPETAS VIRTUALES

a) Para que los usuarios tengan acceso a la información ubicada en las unidades de red o carpetas virtuales y/o compartidas, el jefe inmediato deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar, al Grupo TIC del Club Militar. Los usuarios tendrán permisos de escritura, lectura o modificación de información en las unidades de red, dependiendo de sus funciones y su rol.

b) La información almacenada en cualquiera de las unidades de red o carpetas virtuales y/o compartidas, debe ser de carácter institucional.

c) Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en las unidades de red o carpetas virtuales.

d) Se prohíbe extraer, divulgar o publicar información de cualquiera de las unidades de red, carpetas virtuales o estaciones de trabajo, sin expresa autorización de su jefe inmediato.

e) Se prohíbe el uso de la información de las unidades de red o carpetas virtuales con fines publicitarios, de imagen negativa, lucrativa o comercial.

8.45 ADMINISTRACIÓN DE CONTRASEÑAS

a) La administración, así como la asignación y entrega de las contraseñas a los usuarios deberá seguir el procedimiento de “SOLICITUD ACCESO A SERVICIOS INFORMATICOS”, Código GT-M01-F04.

b) Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

c) Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

d) Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.

e) Las contraseñas no deberán ser reveladas.

f) Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia y se debe realizar un procedimiento de Gestión de Usuarios y Contraseñas.

g) Es deber de cualquier funcionario y tercero reportar cualquier sospecha de que una persona esté utilizando un usuario y contraseña que no le pertenece, acorde con el procedimiento de Gestión de Incidentes.

8.46 BLOQUEO DE SESIÓN, ESCRITORIO LIMPIO

a) En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica, protegida bajo llave.

b) Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.

c) Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por el Grupo TIC del Club Militar.

d) Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo, documentos, accesos directos a los mismos o a sistemas de información sensibles.

e) Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

8.47 CONTROLES CRIPTOGRAFICOS

a) Se deben identificar, definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, de acuerdo con los lineamientos definidos en el procedimiento de Inventario y Clasificación de Activos de Información, tanto cuando se encuentra almacenada como cuando es transmitida o procesada, teniendo en cuenta la clasificación y sensibilidad de la información.

b) No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por la oficina de Informática, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios y terceros autorizados

8.48 GESTIÓN DE VULNERABILIDADES TECNICAS

a) El Grupo gestión TIC, se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

b) El Grupo gestión TIC, será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica del Club Militar.

c) No se permite a los usuarios de los activos informáticos, sin la autorización expresa del Grupo gestión TIC, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos del CLUB MILITAR, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

8.49 CONTROL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

a) Los funcionarios y terceros deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

b) Para los casos en que los incidentes reportados requieran escalamiento a los entes de control y/o judicialización, se deberá coordinar con los organismos que cuentan con función de policía judicial.

c) Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad para el Club Militar.

d) Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo, y de ser posible, la valoración de los daños.

e) Se debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.

f) Los resultados de las investigaciones que involucren a los funcionarios del CLUB MILITAR, deberán ser informados a los Grupos y/o Oficinas de competencia.

g) El Grupo de Gestión TIC, deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

8.50 SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO

a) El Club Militar debe contar con un plan de Continuidad del Negocio que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

b) Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Continuidad de Negocio.

c) Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio

8.51 CONTROL DE PORTAL WEB

a) El Club Militar, debe contar con un plan de gestión del portal Web, que asegure el cumplimiento de la normatividad GEL vigente.

b) La Entidad debe establecer los requerimientos de seguridad, funciones, y responsabilidades relacionados con la publicación de la información en el portal web.

c) El Grupo TIC, asignará claves y usuarios a los funcionarios designados para mantener actualizada la información de cada sección del portal Web.

8.52 SANCIONES

SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores del Club Militar. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

Se consideran como Delitos informáticos, los siguientes conceptos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: o Acceso ilícito a sistemas informáticos. o Interceptación ilícita de datos informáticos. o Interferencia en el funcionamiento de un sistema informático. o Abuso de dispositivos que faciliten la comisión de delitos. Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.
2. Delitos informáticos: o Falsificación informática mediante la introducción, borrado o supresión de datos informáticos. O Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
3. El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.
4. Delitos relacionados con el contenido: o Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
5. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

6. **CÓDIGO PENAL COLOMBIANO**, se estipulan los siguientes artículos:

DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO: El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave, la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA. Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

DE LOS ATENTADOS INFORMATICOS Y OTROS INFRACCIONES

Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción mensual, la sanción allí señalada se incrementará en la mitad.

DE LOS DELITOS CONTRA LOS DERECHOS DE AUTOR

CAPITULO UNICO: DE LOS DELITOS CONTRA DERECHOS DE AUTOR

Artículo 270: Violación a los derechos morales de autor. Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veintiséis puntos sesenta y seis (26.66) a trescientos salarios mínimos legales mensuales vigentes quien: "…3. Por cualquier medio o procedimiento compendie, mutile o transforme sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico…"

8.53 RESPONSABILIDADES LEGALES POR USO INDEBIDO DE LA INTRANET, INTERNET O CORREO INSTITUCIONAL DEL CLUB MILITAR

ALCANCE LEGAL: Ejercerán la vigilancia, aplicación y control del presente procedimiento todos los funcionarios públicos y las personas naturales vinculadas como trabajador oficial, por prestación de servicios u otra modalidad contratada por la entidad ya sea por outsourcing, convenios para apoyar la gestión, pasantes de entidades educativas, celebrados con el Club Militar.

El no cumplimiento de las normas establecidas en la presente resolución, total o parcialmente acarrearan acciones de tipo sancionatorio impuestas por el Club Militar o por la Autoridad competente, de acuerdo a las políticas de seguridad de la información establecidas para el Club Militar y a las decisiones tomadas por el Comité de Seguridad de la información, amparados bajo las normas legales que regulan la seguridad de la información y de la privacidad de la misma en Colombia, dentro de las cuales se encuentran, entre otras, las siguientes:

Ley 524 de 1999, en las cual se establecen que los mensajes de correo electrónico revisten la misma fuerza probatoria que tienen los documentos físicos, en casos de investigaciones de tipo interno, administrativo, judicial o penal.

Ley 679 de 2001, de acuerdo a esta Ley se establece: todas las personas deben prevenir, bloquear, combatir y denunciar la explotación, alojamiento, uso, publicación, difusión de imágenes, textos, documentos, archivos audiovisuales, uso indebido de redes globales de información o el establecimiento de vínculos telemáticos de cualquier clase relacionados con material pornográfico o alusivo a actividades de menores de edad, por cuanto podría generar responsabilidad penal.

La Ley Estatutaria 1266 del 31 de diciembre de 2008, por la cual se dictan disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan disposiciones.

9. ESTRATEGIA GENERAL

Hoy en día las empresas que no entiendan la importancia de la Seguridad Informática y que no inviertan en preservar sus recursos estarán destinadas a la ruina.

La Seguridad Informática aparece en el mundo moderno con el incremento exponencial de la revolución de la información. Los datos son un elemento presente a lo largo de la historia de la humanidad, pero que cobró importancia con la posibilidad de utilizar de manera masiva sistemas informáticos que agilicen el procesamiento y acceso de esa información al estar almacenada digitalmente.

El nivel de riesgo de una vulnerabilidad hace referencia al daño que ella puede causar, sin importar de qué forma actúa.

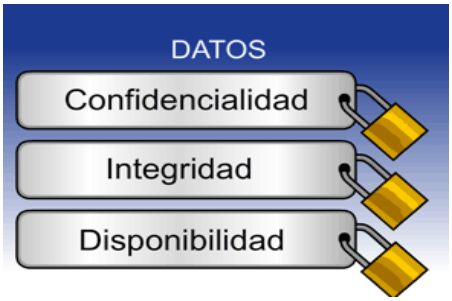
También es importante señalar, que aun cuando las Entidades desarrollen una extraordinaria planificación, juegan un papel de mucha importancia, los organismos internos y externos responsables de auditar los datos generados por los sistemas informáticos. Debe quedar claro, que cada aplicación debe ser revisada y auditada por especialistas en la materia, sería un gravísimo error no considerar la auditoría de los sistemas informáticos oportunamente ya que, no hacerlo, sería extremadamente riesgoso para cualquier evento electoral.

La "Seguridad Informática", es aquella que establece una Entidades electorales deberán asumir la obligación de proteger la transferencia de datos entre sí, puesto que el riesgo de violación de los mismos cada vez se hace más frecuente y notorio dentro de las redes de datos. Por consiguiente, dentro el proceso de planificación, no se debe evitar la seguridad informática, como parte de tareas de mucha importancia y alto riesgo. [2]

La política de seguridad será la guía a seguir en el Club Militar para poder asegurar la información más valiosa garantizando la confidencialidad, integridad y disponibilidad de los datos.

La Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado
La Integridad se refiere a la corrección y completitud de los datos.
La Disponibilidad es asegurar que los datos sean utilizables cuando estos sean necesitados para las tareas habituales de la organización.

Gráfica 1: Los Datos



Fuente: [En línea] Protege tu información. (2012)

En líneas generales, cuando se decide desarrollar una Política de Seguridad estamos estableciendo las bases para la gestión de la seguridad de la información que se procesa en nuestros sistemas informáticos, sin embargo, no sólo estableceremos indicaciones técnicas sino también organizativas, relacionadas con recursos humanos o incluso con la seguridad física del Club Militar.

Hay que tener en cuenta que la seguridad no es sólo un aspecto tecnológico, su Política de Seguridad también debe incluir referencias a concienciación y formación a todos sus empleados, incluyéndolos para la firma de compromisos de confidencialidad por parte de los mismos.

La Política de Seguridad debe cubrir, en la medida de sus posibilidades, todos los aspectos que pudieran poner en peligro su información, no olviden las medidas de seguridad física. ¿De qué le sirve tener un cortafuego y diez sistemas de seguridad que le gestiona un experto técnico si cuando sus empleados se marchan a comer dejan las puertas de su oficina abierta y los PCs sin ningún tipo de protección?[3]

9.1 ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

Con el fin de generar conciencia y mitigación del riesgo que afectan la seguridad de la información se presentan algunas acciones a fin de que se deban evitar:

- Dejar equipos encendidos en horas no laborales.
- Permitir que personas ajenas a la Entidad ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
- No clasificar y/o etiquetar la información.
- No guardar adecuadamente documentos impresos que contengan información clasificada al terminar la jornada laboral.

- Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre la mesa.
- No clasificar y/o etiquetar la información.
- Hacer uso de la red de datos de las Entidad para obtener o difundir material publicitario, comercial (no institucional), así como la distribución de cadenas de correo.
- Instalar software en la plataforma tecnológica de la Entidad cuyo uso no está autorizado por el Grupo Gestión de Sistemas o quien haga sus veces atentando contra las leyes de derechos de autor o propiedad intelectual.
- Enviar información no pública por correo físico, copia impresa o electrónica sin la debida autorización y/o sin utilización de los protocolos establecidos para la divulgación.
- Almacenar y mantener información clasificada en dispositivos de almacenamiento, móviles de cualquier tipo que no sean propiedad de la Entidad.

Usar servicios de Internet en los equipos de la Entidad diferente al provisto por el Grupo Gestión de Sistemas o quien haga sus veces.

Los documentos que sirven de soporte a esta política son:

- INSTRUCTIVO CREACIÓN DE USUARIOS
- PROCEDIMIENTO ELIMINACIÓN PERMISOS DISPOSITIVOS EXTRAIBLES
- PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- PLAN DE CONTINUIDAD DEL NEGOCIO
- FORMULARIO SOLICITUD DE ACCESO A SERVICIOS INFORMATICOS
- COMPROMISO DE CONFIDENCIALIDAD Y USO DE LA INFORMACION

10. VALIDACIÓN DE FIRMAS

ELABORÓ	REVISÓ	APROBÓ
Firma Nombre: Ing. **ROSA ANGELINA MONCADA** Cargo: Coordinador Grupo de Gestión TIC	Firma Nombre: Ing. **ROSA ANGELINA MONCADA** Cargo: Coordinador Grupo de Gestión TIC Firma	Firma Nombre: **VALM (RA) HÉCTOR ALFONSO MEDINA TORRES** Cargo: Director General del Club Militar.

	Nombre: **CN(RA) DANIEL ANTONIO PINZÓN VÁSQUEZ** Cargo: Jefe Oficina de Planeación Firma Nombre: Dra. **JENNY LILIANA SAENZ PARDO** Cargo: Jefe Oficina Asesora Jurídica Firma Nombre: **CR. JOHN FREDY UBAQUE RODRÍGUEZ** Cargo: Subdirector General Club Militar	

REGISTRO DE FIRMAS ELECTRONICAS

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Club Militar

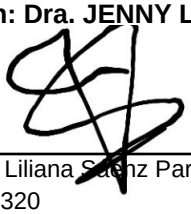
gestionado por: azsign.com.co

Id Acuerdo: 20230313-154748-0b48a9-57390177 Creación: 2023-03-13 15:47:48

Estado: Finalizado Finalización: 2023-03-23 16:33:14

Escanee el código para verificación

Aprobación: Dra. JENNY LILIANA SAENZ PARDO

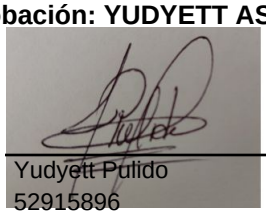


Jenny Liliana Saenz Pardo
52083320
jlsaenz@clubmilitar.gov.co
Jefe Oficina Asesora Jurídica
Club Militar

Aprobación: CN(RA) DANIEL ANTONIO PINZÓN VÁSQUEZ

DANIEL ANTONIO PINZON VASQUEZ
79262110
dapinzon@clubmilitar.gov.co
JEFE OFICINA ASESORA DE PLANEACION
CLUB MILITAR

Aprobación: YUDYETT ASTRID PULIDO GUEVARA



Yudyett Pulido
52915896
yapulido@clubmilitar.gov.co

Aprobación: ING. ROSA ANGELINA MONCADA CASTILLO

ROSA ANGELINA MONCADA CASTILLO
52188084
ramoncada@clubmilitar.gov.co
COORDINADOR TIC
CLUB MILITAR

REGISTRO DE FIRMAS ELECTRONICAS

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20230313-154748-0b48a9-57390177 Creación: 2023-03-13 15:47:48

Estado: Finalizado Finalización: 2023-03-23 16:33:14

Escanee el código para verificación

Aprobación: VALM (RA) HÉCTOR ALFONSO MEDINA TORRES, Director

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

Aprobación: CR. JOHN FREDY UBAQUE RODRÍGUEZ, Subdirector

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

REPORTE DE TRAZABILIDAD

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Club Militar

gestionado por: azsign.com.co

Id Acuerdo: 20230313-154748-0b48a9-57390177 Creación: 2023-03-13 15:47:48

Estado: Finalizado Finalización: 2023-03-23 16:33:14

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Aprobación	ROSA ANGELINA MONCADA CASTILLO ramoncada@clubmilitar.gov.co COORDINADOR TIC CLUB MILITAR	Aprobado	Env.: 2023-03-13 15:47:48 Lec.: 2023-03-13 15:48:09 Res.: 2023-03-13 15:48:37 IP Res.: 200.91.222.50
Aprobación	Yudyett Pulido yapulido@clubmilitar.gov.co	Aprobado	Env.: 2023-03-13 15:48:37 Lec.: 2023-03-13 15:52:38 Res.: 2023-03-13 15:54:09 IP Res.: 200.91.222.50
Aprobación	DANIEL ANTONIO PINZON VASQUEZ dapinzon@clubmilitar.gov.co JEFE OFICINA ASESORA DE PLANEACION CLUB MILITAR	Aprobado	Env.: 2023-03-13 15:54:09 Lec.: 2023-03-13 18:15:41 Res.: 2023-03-13 18:16:15 IP Res.: 200.91.222.50
Aprobación	Jenny Liliana Sáenz Pardo jlsaenz@clubmilitar.gov.co Jefe Oficina Asesora Jurídica Club Militar	Aprobado	Env.: 2023-03-13 18:16:15 Lec.: 2023-03-15 09:18:50 Res.: 2023-03-15 09:42:25 IP Res.: 200.91.222.50
Aprobación	CORONEL JOHN FREDY UBAQUE RODRÍGUEZ asistentesubdireccion@clubmilitar.gov.co Subdirector General	Aprobado	Env.: 2023-03-15 09:42:25 Lec.: 2023-03-15 10:19:09 Res.: 2023-03-15 20:30:50 IP Res.: 200.91.249.34
Aprobación	Vicelamirante (RA) HÉCTOR ALFONSO MED asistentedireccion@clubmilitar.gov.co Director General Club Militar	Aprobado	Env.: 2023-03-15 20:30:50 Lec.: 2023-03-16 10:10:19 Res.: 2023-03-23 16:33:14 IP Res.: 200.91.249.34