CLUB MILITAR

RESOLUCIÓN NÚMERO 000694 **DE 2018**

[24 ABR 2018]

Por la cual se adopta el Manual de Políticas Generales y Específicas de Manejo de Seguridad de la Información para el Club Militar y se dictan otras disposiciones.

EL DIRECTOR GENERAL DEL CLUB MILITAR

En uso de sus facultades legales y en especial las que le confiere el Decreto 444 del 16 de Marzo del 2017 y el Acuerdo número 004 del 9 de marzo de 2001, en concordancia con los dispuesto en el artículo 74 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, y,

CONSIDERANDO

Que la Constitución Política de Colombia 1991, establece el derecho a la intimidad personal.

Que la Ley 527 de 1999, reglamenta el uso del comercio electrónico.

Que la Ley 599 del 2000 Código Penal Colombiano aprueba sanciones por faltas en contra de la seguridad de la información.

Que la Ley 603 del 2000 emite las directrices sobre derechos de autor y control de legalidad del Software.

Que la Ley 734 de 2002 Código Disciplinario Único y determina sanciones a las faltas para los funcionarios públicos que incurran en dichas faltas.

Que en la Ley 1266 de 2008 se dictan disposiciones generales del Habeas Data.

Que la Ley 1273 de 2009 expide normas y disposiciones sobre la Protección de la Información y de los datos.

Que la Ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales.

Que el Decreto reglamentario 1377 del 27 de Junio de 2013. normaliza las disposiciones la Protección de la Información y de los datos.

Que el Ministerio de Tecnologías de la Información para la implementación de la Estrategia de Gobierno digital para las entidades públicas, se encuentra actualmente vigente el Decreto 1499 de 2017.

Que la Norma Técnica Colombiana NTC-ISO/IEC 27000, dicta lineamientos de seguridad de la información.

Que la Directiva No. 2014-18 dicta "POLITICAS DE SEGURIDAD DE LA INFORMACIÒN" para el sector Defensa.

Que el Club Militar es un establecimiento público del Orden Nacional, con personería Jurídica, autonomía administrativa y patrimonio independiente , adscrito al Ministerio de Defensa Nacional, reorganizado conforme a la Ley 489 de 1998 y Decretos Leyes 2336 de 1071 y 2164 de 1984.

Que en mérito de lo expuesto,

RESUELVE

ARTÍCULO 1º. Adopción del Manual. El Club Militar adopta el Manual de Políticas Generales y Específicas de Manejo de Seguridad de la Información el cual se aplicará en todos los niveles de la organización; en las tres Sedes del Club Militar, a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

ARTÍCULO 2º. Objetivo General del Manual, establecer los lineamientos de políticas de Seguridad de la Información necesarios para el manejo de la información y los recursos tecnológicos del Club Militar.

PARAGRAFO PRIMERO: El Manual adoptado en el presente artículo será socializado por el Grupo Gestión TIC´s.

PARAGRAFO SEGUNDO: Es responsabilidad de cada empleado público, trabajador oficial, contratistas, y personal en comisión de las Fuerzas Militares y de la Policía Nacional, conocer, aplicar e implementar las políticas contenidas en el manual.

ARTÍCULO 3º. Contenido del Manual. El Manual de Políticas Generales y Específicas de Manejo de Seguridad de la Información, tendrá el siguiente contenido:

a) INTRODUCCIÓN, OBJETIVOS, ALCANCE, DEFINICIONES, TÉRMINOS, NORMATIVIDAD, GENERALIDADES, ESTRATEGIA GENERAL, MISIONES PARTICULARES, ROLES Y RESPONSABILIDADES.

b) ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN, POLITICAS GENERALES DE MANEJO DE LA INFORMACION, SEGURIDAD EN LA ORGANZACIÓN.

c) GESTIÓN DE ACTIVOS DE INFORMACIÓN,GESTIÓN RECURSO HUMANO,GESTIÓN CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN ,GESTIÓN SEGURIDAD DEL ENTORNO ,GESTIÓN CONTROL DE ACCESO,GESTIÓN DE COMUNICACIONES, GESTIÓN DESARROLLO Y MANTENIMIENTO SISTEMAS DE INFORMACIÓN,GESTIÓN DE CONTINUIDAD DEL NEGOCIO,REQUERIMIENTOS LEGALES.

d) POLITICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÒN ,EN LA GESTION DE TERCEROS,EN LOS ACUERDOS DE CONFIDENCIALIDAD,EN ACUERDOS DE INTERCAMBIO DE INFORMACION Y SOFTWARE DEL USO DE INTERNET,USO DE CORREO ELECTRONICO INSTITUCIONAL O CORPORATIVO,USO DE REDES INALAMBRAICAS,EN SEGMENTACIÒN DE REDES,EN COMPUTACIÒN EN LA NUBE,DERECHOS DE PROPIEDAD INTELECTUAL,CONTROL DE CAMBIOS,CONTROL DE VERSIONES,SEPARACIÒN DE AMBIENTES,RECURSOS TECNOLÓGICOS.

CONCIENTIZACION Y CAPACITACION EN SEGURIDAD DE LA INFORMACION,FINALIZACIÒN DE LA RELACIÒN LABORAL,SEGURIDAD FISICA,SEGURIDAD Y MANTENIMIENTO DE LOS EQUIPOS,SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES,TRASLADO FUERA DE LA ENTIDAD,PROTECCIÒN CONTRA SOFTWARE MALICIOSO,COPIAS DE RESPALDO,GESTIÒN DE MEDIOS REMOVIBLES,COMPUTACIÒN MÓVIL,GESTIÒN DE REGISTROS,LOGS,CONTROL DE ACCESO,SEGURIDAD DEL CENTRO DE DATOS Y CENTRO DE CABLEADO,USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÒN,USO DE UNIDADES DE RED Y CARPETAS VIRTUALES,ADMINISTRACIÒN DE CONTRASEÑAS,BLOQUEO DE SESIÓN, ESCRITORIO LIMPIO,CONTROLES CRIPTOGRÁFICOS,CONTROL DE VULNERABILIDADES TECNICAS,CONTROL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN ,SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO ,CONTROL DEL PORTAL WEB.

e) SANCIONES,DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS,DE LOS ATENTADOS INFORMATICOS Y OTRAS INFRACCIONES,DE LOS DELITOS CONTRA LOS DERECHOS DE AUTOR,RESPONSABILIDADES LEGALES POR USO INDEBIDO DE INTERNET O CORREO INSTITUCIONAL DEL CLUB MILITAR

ARTÍCULO 4º. Aspectos Relevantes. A continuación se relacionan los aspectos más relevantes del Manual y se describen brevemente.

PARAGRAFO PRIMERO. POLÍTICAS DEL MANEJO DE LA INFORMACIÓN:

a) Para la creación y asignación de las cuentas de usuario, usuario de red, cuentas de Correo Electrónico Institucional, perfiles de aplicaciones; se asignarán de manera individual a cada servidor público y se realizará mediante el Formato de calidad denominado "SOLICITUD ACCESO A SERVICIOS INFORMATICOS", Código GT-C01-F04, que se encuentra en la carpeta compartida de calidad de cada equipo unidad Y: /. El cuál debe ser diligenciado en su totalidad, revisado por el Jefe inmediato, autorizado por el Profesional de Apoyo de la Oficina de Planeación y con el visto bueno por el Director General. Adicionalmente se adjuntara el formato de Aceptación de las Políticas de Uso (PUA) con nombres, apellidos completos, número de identificación y huella.
b) 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 Electrónico 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 "ACUERDO DE CONFIDENCIALIDAD PARA TODOS LOS EFECTOS...",
c) Todo el personal debe 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.
d) El personal responsable del manejo de la información y de su seguridad se abstendrá en parte el uso del Internet de la Entidad, la conexión alámbrica a la Red LAN de la Entidad, debe estar autenticando contra el controlador de dominio del Club Militar, 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 inherente al cargo.

e) La Información consultada en cualquier horario de trabajo a través de Internet debe apoyar directamente las funciones relacionadas con el campo de responsabilidad laboral del servidor público y/o servir como herramienta para desempeñar sus funciones.
f) Las políticas y estándares documentan formalmente las reglas para la protección de la información del Club Militar, cuando se utilicen los servicios de Internet y establecen que la información de la entidad debe ser protegida por todos los servidores públicos del Club Militar.
g) Es responsabilidad de los usuarios informar oportunamente acerca de una sospecha de información por un virus, recepción de spam (mensajes de correo no deseado), o comportamiento anómalo por causas desconocidas, a la mesa de ayuda del Grupo Gestión TIC´s; ante estas situaciones de riesgo, deberá abstenerse de usar su computador y desconectarlo físicamente de la red.

PARAGRAFO SEGUNDO. POLITICAS DE PRIVACIDAD DE LA INFORMACIÓN:

a) En cumplimiento de la Ley Estatutaria 1581 de 2012 y el Decreto número 1377de 2013, donde se define el dato personal como el nombre, la edad, el sexo, el estado civil, el domicilio, entre otros, e indica que Los datos van a ser debidamente almacenados en cualquier soporte físico o electrónico y ser tratados de forma manual o automatizada.
b) El Club Militar ordena que los servidores públicos y demás prestadores de servicios bajo cualquier modalidad de contratación de la Entidad, deben cumplir con las políticas de privacidad de la información de los socios del Club Militar, no cediendo, ni divulgando a terceros los datos personales de las bases de datos propias de la Entidad que se recogen a través de archivos planos o vía Web sin su consentimiento expreso. Sin perjuicio de lo anterior, el usuario consiente en divulgar parcial o totalmente los datos personales de los socios de la Entidad, sin su consentimiento expreso.

PARAGRAFO TERCERO.POLITICAS DE USO ADECUADO DEL CORREO INSTITUCIONAL.

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

PARAGRAFO CUARTO.RESPONSABILIDADES POR USO INDEBIDO DEL INTERNET O CORREO INSTITUCIONAL DEL CLUB MILITAR.

a) Ejercerán la vigilancia, aplicación y control por el uso debido del internet o correo institucional del club militar todos funcionarios públicos y las personas naturales vinculadas como trabajador oficial, por prestación de servicios u otra modalidad contratada por la entidad ya sea por outsorcing, convenios para apoyar la gestión, pasantes de entidades educativas, celebrados con el Club Militar.
b) 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.

ARTICULO 5º: Sanciones. Se consideran como delitos Informáticos, los siguientes con sus respectivas sanciones estipuladas dentro del Código Penal Colombiano, así:

DELITO	DESCRIPCIÓN	SANCIÓN
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 transporte.	Según el **CPC** del **Articulo 269C**. Incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
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.	Según el **CPC Articulo 269D:** 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.

000694

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.	Según el **CPC Articulo 269E:** 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.
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.	Según el **CPC Articulo 269F:** 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.
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.	Según el **CPC Articulo 269G:** 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.
CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA	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 quién 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.	Según el **CPC Articulo 269H:** 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.

000601

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.	Según el **CPC Articulo 269I:.**, incurrirá en las penas señaladas en el artículo 240 de este Código.
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.	Según el **CPC Artículo 269J:** 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.
DE LOS DELITOS CONTRA LOS DERECHOS DE AUTOR.	Quién 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..."	Según el **CPC Artículo 270 K:** Violación a los derechos morales de autor. Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veinte seis punto sesenta y seis (26.66) a trescientos salarios mínimos legales mensuales vigentes.

ARTICULO 6º. La presente Resolución rige a partir de la fecha de expedición y deroga las normas y resoluciones que le sean contrarias.

COMUNIQUESE Y CÚMPLASE.

Dada en Bogotá, D.C. a los, 24 ABR 2018

Vicealmirante (RA) **DANIEL IRIARTE ALVIRA**
Director General

V°/B°: CN (RA) RICARDO ARIZA URANGO, Jefe Oficina Asesora de Planeación.
Revisó: Ing. ROSA ANGELINA MONCADA CASTILLO, CGT.
Elaboró: Ing. YENIFER CASTAÑEDA PEDREROS, Asesora oficina de Planeación.