CIRCULAR

No. 0 3 1 0

Bogotá D.C., **10 FEB. 2015**

PARA: Funcionarios y Contratistas Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública – FONDETEC

ASUNTO: Instrucciones de carácter interno y permanente.

De conformidad con lo previsto en la Directiva Permanente del Ministerio de Defensa Nacional No. DIR2014-18, del 19 de junio de 2014, "POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR DEFENSA", se adoptan los lineamientos a seguir para la implementación de las Políticas de Seguridad de la Información, en el Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública – FONDETEC, con el fin de "establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios y aquellas personas que tengan una relación contractual con PAP MINISTERIO DE DEFENSA NACIONAL - FONDETEC o que tenga acceso a los activos de información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información en aras de fortalecer la continuidad de las actividades administrativas, operativas y logísticas del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública – FONDETEC, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información".

A continuación se establecen las políticas de seguridad de la información, así como los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información.

1.1. Uso Adecuado de los Activos de Información

El Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, podrá monitorear y supervisar la información, sistemas, servicios y equipos que sean de su propiedad, de acuerdo con lo establecido en esta política y la legislación vigente.

1.1.1 Internet

a. La navegación en Internet estará controlada de acuerdo con las categorías de navegación definidas para los usuarios; sin embargo, en ningún caso se consideraran aceptables los siguientes usos:

1. Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

2. Publicación, envío o adquisición de material sexualmente explícito, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.

3. Publicación o envío de información confidencial hacia afuera del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.

4. Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados.

5. Publicación de anuncios comerciales o material publicitario, salvo las áreas que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el Jefe o Coordinador del Área.

6. Promover o mantener asuntos o negocios personales.

7. 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.

8. Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la Entidad.

9. Uso de herramientas de mensajería instantánea no autorizadas por el Área Administrativa - Servicios de Tecnología de Información y Comunicación, o la que haga sus veces.

10. Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.

b. Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios y terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

c. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

1.1.2 Correo electrónico institucional o corporativo:

a. La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones o actividades asignadas dentro de cada una de las Áreas del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública.

b. Los mensajes y la información contenida en los buzones de correo institucional son de propiedad del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública. Cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información y el tráfico de la misma, se considera de interés del Fondo.

c. El tamaño de los buzones y mensajes de correo serán determinados por el Área Administrativa - Servicios de Tecnología de Información y Comunicación, o la que haga sus veces, de las respectivas Áreas que conforman el Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, conforme a las necesidades de cada usuario y previa autorización del Jefe inmediato.

d. El Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública suministrará una cuenta de correo corporativa por cada Área que lo requiera, la cual será utilizada para el envío masivo de correos institucionales.

e. No se considera aceptado el uso del correo electrónico corporativo para los siguientes fines:

1. Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

2. El envío de cualquier tipo de archivo que ponga en riesgo la seguridad de la información; en caso que sea necesario hacer un envío de este tipo de archivos deberá contar con la autorización correspondiente por parte del Área Administrativa - Servicios de Tecnología de Información y Comunicación, o la que haga sus veces.

3. El envío de información relacionada con la Defensa y la Seguridad Nacional a otras entidades del Gobierno diferentes a las que conforman el Sector Defensa, sin la autorización previa del propietario de la información y de la Dirección del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública.

f. Toda información que requiera ser transmitida fuera del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables y con mecanismos de seguridad. Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

g. Todo correo electrónico deberá respetar el estándar de formato e imagen corporativa definido por el Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública y deberá contener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:

1. El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.

2. El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.

3. En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.

4. Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

1.1.3 Redes Inalámbricas:

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 las redes institucionales.

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. El servicio de Internet en las Regionales, deberá contar con mecanismos de autenticación de usuarios y deberá estar configurado de tal manera que permita el desarrollo de las actividades académicas y de investigación.

d. El servicio de internet en las Regionales, deben estar configuradas de forma independiente a la red operativa del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública.

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

1.1.4 Computación en la Nube (Cloud Computing)

a. Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos como son (Google Drive, Google Talk, Google Calendar, Google Docs, SkyDrive, Dropbox, Box, Mega, Amazon Web Services, etc.).

b. Ningún servicio de carácter operativo e institucional del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, deberá ser contratados en servicios en la nube públicos o híbridos.

c. Para el caso de las Regionales, se podrá hacer uso de servicios en la nube públicos e híbridos, siempre y cuando no se vea comprometida la seguridad institucional o información clasificada.

d. El Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, podrá implementar servicios de nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

1.1.5 Sistemas de Información de Acceso Público

a. La información pública producida por el Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.

b. El portal institucional, deberá contener la política de privacidad y uso, así como la política de seguridad del mismo.

c. El Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, deberán garantizar el derecho de Habeas Data al público que hace uso del servicio del portal institucional y propender por la seguridad de la información ingresada a través de él, aclarando que no se es responsable de la veracidad de la misma.

d. Toda la información publicada en el portal del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, deberá contar con la

revisión y aprobación de la Dirección del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, y deberá estar debidamente rotulada según su nivel de clasificación.

1.1.6 Recursos tecnológicos:

a. La instalación de cualquier tipo de software en los equipos de cómputo del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública es responsabilidad exclusiva del Área Administrativa - Servicios de Tecnología de Información y Comunicación, o las que hagan sus veces, por tanto son los únicos autorizados para realizar esta labor.

b. Ningún activo de información debe ser instalado con la configuración establecida por defecto por el fabricante o proveedor, incluyendo cuentas y claves de administrador.

c. Los funcionarios o contratistas 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 el Área Administrativa - Servicios de Tecnología de Información y Comunicación o la que haga su veces, del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública.

d. Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser realizadas por el Área Administrativa - Servicios de Tecnología de Información y Comunicación o quien haga sus veces.

e. Los equipos de cómputo asignados, deben ser devueltos al Área Administrativa - Servicios de Tecnología de Información y Comunicación o la que haga su veces, una vez sean reemplazados o cuando el funcionario o contratista de dicho equipo finalice su vinculación con el Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, para que le sea expedido el Paz y Salvo.

f. De acuerdo con el literal anterior, el área no debe almacenar equipos de cómputo una vez haya cesado el uso de los mismos.

1.1.7 Uso de recursos informáticos:

a. Se considera que está incurriendo en una falta grave o incumplimiento de sus obligaciones, el funcionario o contratista que destruya o dañe los equipos informáticos que se le hayan asignado para realizar su labor o actividad o cuando manipule cualquier otro equipo del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública de forma indebida, así como realizar la manipulación maliciosa de los recursos informáticos que puedan originar daños en los servidores, equipos pc, equipos de comunicaciones, estructura de red, base de datos, servicio de internet, el correo electrónico y los servicios y/o recursos informáticos asociados.

b. Los usuarios no deben manipular comidas, bebidas o fumar cerca de los equipos informáticos que puedan originar directa o indirectamente su mal funcionamiento, siendo responsable el funcionario o contratista por el deterioro del mismo, en estos casos el Área Administrativa - Servicios de Tecnología de Información y Comunicación o las que hagan sus veces, informarán mediante documento a la Dirección de FONDETEC, para que ésta determine las acciones a seguir.

1.1.8 Ingreso y salida de equipos:

a. Todo equipo informático (Computador Portátil, PC, Impresoras, Scanner, Lectoras Digitales, Video-beam, etc.) de propiedad del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, que salga o ingrese a las instalaciones de FONDETEC, debe contar con el formato correspondiente para tal fin, debidamente diligenciado y autorizado por el Área Administrativa - Servicios de Tecnología de Información y Comunicación o la que haga su veces.

b. Los equipos Informáticos que se asignan a los funcionarios o contratistas del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, que salen a comisión son de uso temporal, estos deben ser

reintegrados al Área Administrativa - Servicios de Tecnología de Información y Comunicación o la que haga su veces, una vez finalice la comisión.

c. El uso de los recursos informáticos (Equipos de Cómputo, Aplicaciones, Sistemas, Bases de Datos, Documentos Digitales, etc.) asignados a los funcionarios o contratistas de FONDETEC, son netamente para asuntos relacionados con las labores administrativas, operativas y logísticas del Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública, siendo el uso personal limitado.

d. El personal de vigilancia, debe realizar el registro en la minuta de control de ingreso y salida de todo equipo informático (Computador Portátil, PC, Impresoras, Scanner, Lectoras Digitales, Video-beam, etc.) quienes deberán exigir la presentación del formato correspondiente para tal fin, debidamente diligenciado y autorizado por el Área Administrativa - Servicios de Tecnología de Información y Comunicación o la que haga su veces.

Cordialmente,

CLAUDIA XIMENA LÓPEZ PAREJA
Directora Fondo de Defensa Técnica y Especializada de los Miembros de la Fuerza Pública - FONDETEC.

Proyecto: Jose P. Bravo Bermejo
Reviso: Jose Guavita Huerfano.

Fondetec
Calle 26 A No. 13-97
Local 11 Bulevar Tequendama
PBX: 7458115
www.fondetec.gov.co
fondetec@mindefensa.gov.co