FUERO MILITAR POLICIAL
DIRECCION LOGISTICA
OFICINA SISTEMAS
MAYO 2017

# DIRECTIVA QUE ESTABLECE EL USO CORRECTO DE EQUIPOS INFORMATICOS Y SERVICIOS DE RED, INTERNET Y CORREO ELECTRONICO EN EL FUERO MILITAR POLICIAL.

**DIRECTIVA Nº 013 /FMP/DE/OF. SISTEMAS.**

## 1. OBJETIVO

Establecer y Normar internamente el uso correcto de los equipos de cómputo, servicios de red, internet y correo electrónico institucional del Fuero Militar Policial.

## 2. ALCANCE

La presente Directiva, es de aplicación y cumplimiento obligatorio, bajo responsabilidad, para todo el personal que labora en las dependencias (Órganos Jurisdiccionales, Fiscales, Administrativos, de Apoyo y Tribunales Superiores Militares Policiales), que conforman el Fuero Militar Policial a nivel nacional.

## 3. CONSIDERACIONES GENERALES

Las tecnologías de información y de comunicación (TICS), con la que cuenta el Fuero Militar Policial, tiene como finalidad servir de apoyo a las labores Jurisdiccionales y Fiscales.

La presente Directiva está orientada a que las TICS, del Fuero Militar Policial, sean utilizadas de manera adecuada por el personal que labora en esta institución, a fin de cumplir con los logros, objetivos y metas institucionales.

## 4. REFERENCIA (BASE LEGAL)

- Constitución Política del Perú
- Ley Nº 30096, Ley de Delitos Informáticos, modificada por la Ley Nº 30171.
- Ley Nº 29182 – Ley de Organización y Funciones del Fuero Militar Policial
- Ley Nº 28612 – Ley que norma el uso, adquisición, adecuación del software en la administración pública.
- Ley Nº 27444 – Ley del procedimiento Administrativo General.

- Decreto Legislativo Nº 1129, Decreto Legislativo que regula elSistema de Defensa Nacional.
- Resolución ministerial Nº 246-2007-PCM, aprueba "Norma Tecnica Peruana NTP-ISO/IEC 17799:2007 EDI Tecnología de la Información Código de Buenas Prácticas para la Gestión de la Seguridad de la Información – Segunda Edición.
- Resolución Ministerial Nº 004-2016-PCM, Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial Nº 246-2007-PCM, Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la Información. 2da Edición", en toda las entidades integrantes del Sistema Nacional de Informática.
- Resolución ministerial Nº 073-2004-PCM, Guía para la Administración Eficiente del Software Legal en la Administración Pública.
- Resolución Jefatural Nº 386-2002-INEI, que aprueba la Directiva Nº 016-2002-INEI/DTNP "Normas Técnicas para el almacenamiento y respaldo de la información procesada por las Entidades de la Administracion Pública.
- Resolución Jefatural Nº 347-2001-INEI, que aprueba la Directiva "Normas y procedimientos técnicos para garantizar la seguridad de la información publicada por las Entidades de Administración Pública.
- Resolución Jefatural Nº 088-2013-INEI, que aprueba la Directiva "Normas para el uso de Servicios de correo electrónico en las Entidades de Administración Pública.
- Resolución Administrativa Nº 126-2011-FMP/TSMP/SG – Reglamento de la Ley Nº 29182.
- Resolución Administrativa Nº 001-2011-PCEFMP-SG, que aprueba el Reglamento de Organización y Funciones del Fuero Militar Policial.
- Sistema de Gestión de Seguridad de la información (ISO 27001).
- COBIT 5.1 (Control Objetives for information and related Technology).
- Ley Nº 30171, Ley que modifica la Ley Nº 30096, Ley de delitos informáticos y su Reglamento.

## 5. SITUACION GENERAL

Los servicios de acceso a Internet, red, recursos de información digital y correo electrónico están disponibles en el Fuero Militar Policial, para facilitar la comunicación institucional y el flujo de información de carácter académica, laboral y de investigación, dentro de los límites que establece la normatividad legal.

Con la presente Directiva se establece las normas requeridas para el buen uso de los equipos de cómputo y para la asignación de accesos y usos de los servicios de red, internet, correo electrónico institucional y aplicativos informáticos.

## 6. FINALIDAD

1) Normar el procedimiento para el uso de los servicios informáticos, así como las medidas de seguridad informática que deberán cumplir las Unidades Orgánicas, para evitar el daño, perdida o mal empleo de la información y material de cómputo y garantizar la seguridad de la red y de los sistemas informáticos del Fuero Militar Policial.

2) Lograr que el personal (Usuarios), comprendan la importancia del buen uso de los servicios de información, entendiendo los beneficios que se obtienen, así como las consecuencias del no cumplimiento de las normas y recomendaciones.

3) Dictar las normas que establecen los procedimientos para la utilización de los servicios informáticos, así como las medidas de seguridad informática que deberán cumplir las Unidades orgánicas, para evitar el daño, perdida o mal empleo de la información y material de cómputo del Fuero Militar Policial.

4) Lograr que los usuarios comprendan la importancia del buen uso de los servicios de información, entendiendo los beneficios que se obtienen, así como las consecuencias del no cumplimiento de las normas y recomendaciones.

5) Las disposiciones contenidas en la presente Directiva, son de competencia de todo el personal que labora en el Fuero Militar Policial (Tribunal Supremo y Tribunales Superiores).

## 7. EJECUCION

Con la presente directiva el Fuero Militar Policial, establece la importancia del manejo de información mediante herramientas tecnológicas, específicamente la informática. Ante esta realidad y consecuentemente a los nuevos retos y amenazas; nuestra institución ha planteado lo siguiente:

## a. DISPOSICIONES GENERALES

1) La Oficina de Sistemas del Fuero Militar Policial es responsable de brindar el soporte necesario para el buen funcionamiento de los equipos de cómputo y servicios informáticos, de manera eficaz y eficiente. Asimismo, es responsable de aprobar la incorporación de tecnologías de información vinculadas con el desarrollo y operación de los sistemas de información y el mantenimiento de los equipos de cómputo asignados a los usuarios.

2) Los usuarios son responsables del cuidado físico y lógico de sus equipos de cómputo, por lo que no deben manipular alimentos, fumar sobre los equipos de cómputo, instalar software o cualquier otra actividad que puedan dañar los equipos o alterar su correcto funcionamiento.

3) Los usuarios son responsables de las actividades que realicen con sus accesos, como su identificación de usuario y contraseña de los servicios informáticos; en caso el usuario ceda su acceso al servicio informático a otra persona, seguirá siendo responsable de las actividades que este tercero realice.

4) El equipo de cómputo que es entregado al usuario, contiene el software base necesario para satisfacer sus funciones y está instalado de acuerdo al perfil solicitado por su Unidad Orgánica; cualquier necesidad adicional debe ser solicitada formalmente a la Dirección Ejecutiva - Oficina de Sistemas del Fuero Militar Policial.

5) No está permitido intercambiar el equipo de cómputo que le ha sido asignado por la institución, bajo responsabilidad.

6) El usuario está terminantemente prohibido de abrir los equipos de cómputo o periféricos, así como de sacar o cambiar componentes periféricos de los mismos. Esta acción será reportada por la Oficina de Sistemas a la Dirección inmediata solicitando la acción disciplinaria correspondiente.

7) Ningún usuario, podrá desarmar, cambiar accesorios, cambiar la configuración de los equipos informáticos que es de responsabilidad del área de mantenimiento y soporte técnico de la Oficina de Sistemas del Fuero Militar Policial.

8) Los Usuarios de computadoras portátiles y proyectores multimedia, por ningún motivo pueden sacar fuera de la institución, salvo para cumplir con funciones de interés institucional, para lo cual deben contar con el permiso respectivo firmado por la Dirección Ejecutiva mediante la Oficina de Bienes Patrimoniales y la Oficina de Sistemas.

9) La Dirección Ejecutiva a través de la Oficina de Sistemas y personal encargado de la administración de Red del Fuero Militar Policial, es responsable de la instalación, configuración, operación y administración de todos los servicios de Red del Fuero Militar Policial, así como el establecimiento de políticas de seguridad de información.

10) El Fuero Militar Policial, no se hace responsable por los conceptos emitidos por los usuarios a través de la Red o por el uso mal intencionado o ilegal, así como por el daño causado a terceros por el uso no apropiado de los servicios habilitados a los usuarios.

11) El usuario que recibe los servicios informáticos solicitados o necesarios para su desempeño, es responsable del cumplimiento de las normas vigentes, del uso adecuado de los equipos de cómputo, del software utilizado, de los datos administrados, así como el cuidado de manuales y otros elementos de soporte que se le entreguen.

## b. DISPOSICIONES COMPLEMENTARIAS

### 1. SOBRE LOS EQUIPOS DE CÓMPUTO

(a) El Usuario es responsable del equipo informático asignado a su cargo (CPU, monitor, impresora, etc.), así como del cuidado de manuales y otros elementos de soporte que se le entreguen.

(b) El usuario está terminantemente prohibido abrir los equipos de cómputo o periféricos, sacar o cambiar componentes internos de los mismos. Esta acción será reportada por la Oficina de Sistemas a la Dirección inmediata, solicitando la acción disciplinaria correspondiente.

(c) Los equipos informáticos (computadoras, impresoras, proyectores multimedia y demás accesorios) serán utilizados exclusivamente para trabajos de fines institucionales, quedando prohibido el uso para fines particulares o de terceros.

(d) El usuario es responsable de organizar y mantener el orden de la información contenida en el equipo de cómputo que la institución le haya asignado.

(e) El usuario que instale algún software en su equipo de cómputo y sea responsable del mal funcionamiento del mismo, generando problemas a los demás equipos conectados a red y de las licencias de software instalado, será responsable de los daños que ocasione.

(f) El usuario no debe alterar el Hardware y Software que se encuentra a su disposición, asimismo no debe cambiar la configuración de los equipos de cómputo determinada por la Oficina de Sistemas.

(g) El personal de la Oficina de Sistemas, es el único autorizado para realizar instalaciones y/o modificaciones a las configuraciones al Hardware y Software de los equipos de cómputo. Asimismo son los autorizados para trasladar los equipos de la institución.

(h) El personal de la Oficina de Sistemas, poseerá una "Clave de Administrador" para poder acceder y/o cambiar las configuraciones de los equipos, ante la necesidad justificada, previa solicitud y autorización del área responsable.

(i) El usuario deberá verificar, al inicio de las labores, que el equipo asignado esté completo y en estado operativo. Informándose de inmediato a la Oficina de Informática sobre cualquier novedad.

(j) En caso de interrupción del fluido eléctrico, no manipular los botones de encendido ni mover los controles internos del equipo.

(k) El usuario que requiera otro software adicional al pre-instalado o acceso a un servicio informático en su equipo debe solicitarlo a la Oficina de Sistemas.

(l) La pérdida de equipos informáticos como consecuencia de la negligencia del usuario responsable será sancionada administrativamente y deberá reponer por otro de iguales o superiores características técnicas.

2. **DEL ACCESO A LA RED**

(a) La Oficina de Sistemas proporcionará acceso a la Red únicamente a los empleados públicos que indique el jefe de área correspondiente, asignándole un nombre de usuario.

(b) El acceso a la Red y demás servicios informáticos (SIAF, Correo electrónico, internet, etc.), podrán ser eliminados a pedido del Jefe de área o cuando la Dirección de Recursos Humanos comunique el cese de determinado empleado.

(c) Solo se podrá utilizar software de navegación web designado por la Entidad.

(d) El acceso a internet será exclusivamente para fines laborales, fines de investigación y fines académicos (Áreas determinadas).

(e) Queda terminantemente prohibido.
- Las conversaciones en tiempo real (chat).
- Descargas de programas, juegos, música y videos.
- El uso de internet para fines particulares o a favor de terceros.
- El uso de redes sociales (Facebook, LinkendIn, Twitter, YouTube, Google+, WatsApp, Instagram, HI5, SoundCloud, Line, Pinterest, Tunbir., Netlog, TWOO, Weibo, Sporify, Snapchat, Slideshare, Askfm, Orkuto, Badoo, Scribd, Myspace, etc.). se encuentra restringido y el acceso a alguna de estas se autorizara por tiempo determinado, previo informe del jefe de área sobre el motivo por el cual solicita el uso de este servicio.
- Acceder a páginas web que incluyan material pornográfico.

(f) Todo trabajo de cableado estructurado, será realizado por la Oficina de Sistemas, a través del área de redes.

(g) Ningún usuario está autorizado a hacer cambios o modificaciones al cableado estructurado, a las direcciones IP, nombres de grupos o nombres de computadoras, y/o equipos asignados a su cargo.

(h) El uso de correo distinto al institucional (Hotmail, Yahoo, Gmail, etc.), se encuentra restringido y el acceso a alguna de estas quedara sujeto a la necesidad del trabajo que realiza el usuario en la institución, previo informe del jefe de área sobre el motivo por el cual solicita el uso de este servicio.

3. **DE LA INFORMACION Y SEGURIDAD**

(a) El nombre de usuario y contraseña es de uso exclusivo del propietario de la cuenta, por lo que está es intransferible, quedando prohibido que el propietario comparta su cuenta y su contraseña.

(b) Para las contraseñas se recomienda claves largas, complejas y que contengan letras, números, signos de puntuación y símbolos. Evitar el uso de nombres, apellidos, números de DNI, ciudades, mascotas, entre otros. (Ejemplo "Tengo1clave+segura").

(c) El usuario deberá bloquear la pantalla de su PC cuando no haga uso de su computadora.

(d) El usuario deberá cerrar las aplicaciones informáticas, salir del acceso de red y apagar su computadora al culminar la jornada laboral o cuando se tenga que ausentarse de su puesto.

(e) En caso que se requiera acceder a la computadora del usuario ausente, el responsable del área correspondiente, deberá solicitarlo por escrito o vía correo electrónico a la Oficina de Sistemas, que se encargara de asignar nuevas claves de encendido y acceso a la red, las que serán de conocimiento exclusivo del responsable de área y el usuario al retorno de su ausencia deberá modificar su clave.

(f) La información almacenada y procesada mediante recursos informáticos del Fuero Militar Policial, así como los aplicativos desarrollados por este último, le pertenecen a la entidad de manera exclusiva y excluyente. Por lo tanto está prohibido el retiro parcial o total de la información, aplicativo o utilidad, almacenado, procesado o desarrollado mediante los recursos informáticos de la entidad.

(g) El usuario es responsable de salvaguardar la información de su equipo y su trabajo realizado, gestionando copias de seguridad necesarias a fin de evitar extravío de información.

(h) Los usuarios no deben consentir a personal ajeno y/o que no sea trabajador directo del Fuero Militar Policial, utilice los equipos de cómputo, y/o recursos informáticos.

## 4. CANCELACION DE PERMISOS

La Oficina de Sistemas, podrá cancelar permisos otorgados a los usuarios si se detecta mal uso de los accesos otorgados, informando directamente a la Dirección Ejecutiva del Fuero Militar Policial.

## 5. DE LA ADQUISICION DE EQUIPOS INFORMATICOS

(a) Los requerimientos para la adquisición de equipos informáticos solicitados, será tramitado a través de la Oficina de Sistemas del Fuero Militar Policial, quien es responsable de aprobar y verificar las especificaciones técnicas de hardware, software o tecnologías de información que se encuentren vinculadas con el desarrollo y operación de los sistemas de información y el mantenimiento de los equipos de cómputo asignados a los usuarios.

(b) Todo pedidos de software y/o actualizaciones de software se presentarán a través de la Oficina de Sistemas.

(c) La Oficina de Sistemas será encargada de salvaguardar todas las licencias de software original, CD-ROM, DVD-ROM, etc., y la documentación al recibir el software nuevo.

(d) La Oficina de Abastecimiento o adquisiciones del FMP, para la adquisición de equipos informáticos, coordinará con la Oficina de Sistemas, para la formulación de las bases a los procesos de selección.

## 8. INSTRUCCIONES ESPECIALES

### 8.1. Instrucciones de Coordinación

#### 8.1.1 DIRECCION EJECUTIVA

La Dirección Ejecutiva, realizará la supervisión, control y cumplimiento de la presente Directiva.

#### 8.1.2 DIRECCION LOGISTICA

La Dirección Logística, a través de la Oficina de Sistemas, será la responsable de llevar a cabo la difusión e implementación de la presente Directiva, así como proponer su actualización según se requiera. Igualmente, supervisará el cumplimiento de la presente disposición.

#### 8.1.3 DIRECCION DE RECURSOS HUMANOS

En caso de cese, cambio de empleo o finalización definitiva del contrato de un empleado (Usuario), la Dirección de Recursos Humanos mediante la Oficina de Personal, comunicará a la Dirección Logística y Oficina de Sistemas, tal situación a fin que se proceda a cancelar todos los accesos otorgados y garantizar la seguridad de la información.

### 4.2. Acuse Recibo

Formato de acuse recibo del Anexo "a".

### 4.3. Tiempo de Vigencia

Entra en vigencia: Al día siguiente de su publicación en el Portal Institucional del Fuero Militar Policial.

## 4.4. Otras Instrucciones

Cualquier modificación posterior al contenido de esta Directiva, se efectuará con documentación complementaria, remitiendo copia a los Organismos correspondientes.

FUERO MILITAR POLICIAL
Director Ejecutivo

FUERO MILITAR POLICIAL
PRESIDENCIA

**Juan Pablo RAMOS ESPINOZA**
General de Brigada EP. (R)
Presidente del Fuero Militar Policial

**Anexos:**
Anexo "A": Glosario de Términos.
Anexo "B": Lista de Distribución.
Anexo "C": Formato para Acuse Recibo.

**ANEXO A**: Glosario de Términos a la **DIRECTIVA Nº 013/FMP/DE/OF. SISTEMAS**

1. **ADMINISTRADOR DE LA RED:** Persona o personas encargadas de la Seguridad de la Red y de asignar los derechos de acceso adecuado a la Red y a las claves de acceso a los usuarios; los mismos que tienen a su cargo el mantenimiento del software y hardware de la red.

2. **ANTIVIRUS:** Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.

3. **BACKUP:** Copia de seguridad total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento.

4. **CORREO ELECTRONICO:** Es el medio por el cual se pueden recibir y enviar información a través de un dispositivo electrónico.

5. **DISCO DURO:** Dispositivo magnético, que almacena todo los programas y datos de la computadora; conserva la información aún con la pérdida de energía, empleando un sistema de grabación magnética digital.

6. **DISPOSITIVO DE ALMACENAMIENTO:** Todo aparato que se utilice para grabar los datos de la computadora en forma permanente o temporal.

7. **DOMINO DE INTERNET:** Es una red de identificación, asociada a un grupo de dispositivos o equipos conectados a la red de internet (Usuario@fmp.gob.pe).

8. **COMPUTADORA PERSONAL O ESTACION DE TRABAJO:** Computadora asignada a los usuarios para el desarrollo exclusivo de las tareas encomendadas del Fuero Militar Policial.

9. **HARDWARE:** Comprende todas las partes físicas y tangibles de la computadora.

10. **SOFTWARE:** Conjunto de programas y rutinas que permiten a la computadora, realizar determinadas tareas.

11. **RED INFORMATICA:** Grupo de computadoras, que comparten información a través de tecnología de cable o inalámbrica.

12. **SERVIDOR:** Equipo informático, que forma parte de una red y provee servicios a otros equipos clientes.

13. **INTERNET:** Conjunto descentralizado de redes de comunicación interconectadas, que utilizan los protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen, funcionen como una red logia única, de alcance mundial.

14. **USUARIO (USER):** Es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático.

15. **CORTAFUEGOS (FIREWALL):** Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

16. **DISPOSITIVOS PERIFERICOS:** Se consideran periféricos a las unidades o dispositivos de hardware a través de los cuales la Computadora comunica con el exterior, y también a los sistemas que almacenan o archivan la información, sirviendo de memoria auxiliar de la memoria principal (Monitor, mouse, impresora, etc.).

17. **ARCHIVO COMPARTIDO:** Un archivo compartido es una propiedad de un archivo informático que tiene la característica de poder ser accedido o manipulado por múltiples personas, computadoras, sesiones o programas. Es un tipo de recurso compartido.

18. **FIRMA DIGITAL:** Es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

19. **SISTEMA OPERATIVO:** Un Sistema Operativo (SO) es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario (Windows, Linux, Mac, Android, etc.).

20. **HACKER:** Es aquella persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

21. **TELEFONIA IP:** Básicamente VoIP es un método por el cual tomando señales de audio analógicas del tipo de las que se escuchan cuando uno habla por teléfono se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección IP determinada.

**ANEXO B**: LISTA DE DISTRIBUCION a la **DIRECTIVA Nº** 013 **/FMP/DE/OF. SISTEMAS**

**DISTRIBUCION:**

1. Presidencia..... 01
2. Secretaria General..... 01
3. Inspectoria General del FMP..... 01
4. Sala de Vocales..... 01
5. Fiscalías FMP..... 03
6. Dirección Ejecutiva..... 01
7. Dirección de Administración y Finanzas.... 01
8. Dirección de Logística..... 01
9. Dirección de Recursos Humanos..... 01
10. Oficina de RRPP e Imagen..... 01
11. CAEJM..... 01
12. Organo de Control Institucional..... 01
13. Defensoría de Oficio..... 01
14. TTSSMMPP..... 05/20

FUERO MILITAR POLICIAL
Director Ejecutivo

FUERO MILITAR POLICIAL
PRESIDENCIA

**Juan Pablo RAMOS ESPINOZA**
General de Brigada EP. (R)
Presidente del Fuero Militar Policial