

2010

Instituto de Previsión Social de la Fuerza Armada



Gerencia General
Unidad de Informática.

**POLÍTICAS PARA EL USO ADECUADO
DE LA TECNOLOGÍA INFORMÁTICA
INSTITUCIONAL.**

Contenido

	<i>No. de Pág.:</i>
I. Políticas.....	1
A. Relacionada a los equipos.....	1
B. Para la solicitud de requerimientos.....	3
C. Mensajería y correo electrónico.....	3
D. Faltas y sanciones a los usuarios.....	7
E. Red institucional.....	8
F. Internet.....	11
II. Misceláneos.....	12

I. POLÍTICAS

A. RELACIONADA A LOS EQUIPOS

1.0 USO DE EQUIPOS Y RECURSOS INFORMÁTICOS.

- 1.1 Para hacer uso del equipo y recurso informático asignado, el usuario debe ser empleado activo del IPSFA.
- 1.2 El uso de Internet debe ser únicamente para fines institucionales, definiéndose como institucionales a todas aquellas búsquedas de información que apoyen el trabajo del usuario.
- 1.3 El uso de equipo de digitalización de documentos (scanners) e impresoras es exclusivamente para actividades institucionales.
- 1.4 Para alargar la vida útil del equipo, se prohíbe ingerir alimentos y bebidas sobre el mismo, así como el fumar cerca del equipo informático.
- 1.5 Se recomienda a los usuarios almacenar los archivos de trabajo en las carpetas institucionales asignadas para cada área o unidades del IPSFA, para evitar cualquier pérdida de información valiosa.
- 1.6 El contenido de los discos duros de las estaciones de trabajo debe ser continuamente depurado para evitar la saturación de espacio. Será responsabilidad del usuario el respaldar la información.
- 1.7 La Unidad de Informática se reserva el derecho de revisión del contenido de lo almacenado dentro del equipo del usuario con el objetivo de velar por el correcto uso del recurso asignado.
- 1.8 Cualquier uso que cause efectos opuestos a la operación de la unidad de informática o ponga en riesgo el uso o rendimiento de la plataforma informática Institucional, será analizado por la jefatura de la unidad para tomar medidas correctivas y preventivas a nivel técnico y/o administrativo según sea el caso.



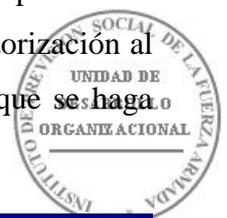
- 1.9 El equipo y recursos asignados se entregarán en buenas condiciones. En caso de extravío o daño de equipo por parte del usuario, se informara a la administración del IPSFA para que se determinen responsabilidades y/o las acciones a seguir.
- 1.10 El personal de la Unidad de Informática es el único autorizado de desconectar, mover, abrir el equipo y sus componentes.
- 1.11 Para eventos especiales que requieran el uso de recurso informático en específico y del cual no dispongan: El Departamento o Unidad interesada deberá solicitarlo por escrito o por correo electrónico, a la Unidad de Informática, con un mínimo de dos días de anticipación.

2.0 TRASLADOS O CAMBIOS DE EQUIPO INFORMÁTICOS

- 2.1 Todas las áreas del IPSFA deberán informar a la Unidad de Informática de todo traslado o cambios del personal con equipo informático asignado, con el objetivo de garantizar la seguridad de los sistemas, modificando y/o inhabilitando los diferentes accesos (correo electrónico, red institucional, a los aplicativos, etc.)
- 2.2 Todas las áreas del IPSFA deberán informar a la Unidad de Informática de todo traslado o cambios del equipo informático asignado a las áreas del IPSFA, a efectos de que sea la Unidad de Informática quién realice el traslado de dicho equipo garantizando su instalación, funcionamiento y actualización de su nueva ubicación tanto en los controles propios de la Unidad de Informática como en los del área de activo fijo.
- 2.3 Todas las áreas del IPSFA deberán informar a la Unidad de Informática, que si poseen equipo sin personal asignado en el área, este deberá ser entregado a la Unidad de Informática para su reubicación en otra área del Instituto donde se necesite.

3.0 PARA EL USO DEL EQUIPO INFORMÁTICO EXTERNO

- 3.1 Si se ingresa un equipo informático a las Instalaciones, que no sea propiedad del IPSFA, y se desea conectar a la red institucional, se deberá solicitar autorización al Jefe de la Unidad de Informática; por un área o persona del IPSFA, que se haga responsable de tal situación.



B. PARA LA SOLICITUD DE REQUERIMIENTOS

1. Todo requerimiento y modificación a los diferentes aplicativos deberá ser solicitado a la Unidad e Informática a través del responsable del mismo, apoyándose del formulario Solicitud y Análisis de Requerimientos. (FORM-08-GG-INF-01) o por medio de correo electrónico dirigido a helpdesk@ipsfa.com, ningún usuario podrá solicitar modificaciones a los aplicativos si no es por medio del responsable del mismo.
2. Todo requerimiento de acceso a los diferentes aplicativos deberá ser solicitado a la Unidad e Informática a través del responsable del mismo, apoyándose del formulario Solicitud y Análisis de Requerimientos. (FORM-08-GG-INF-01) o por medio de correo electrónico dirigido a helpdesk@ipsfa.com, ningún usuario podrá solicitar accesos a los aplicativos si no es por medio del responsable del mismo.
3. Todo requerimiento de Internet y Software de Mensajería deberá ser solicitado a la Unidad e Informática a través del responsable del mismo, apoyándose del formulario (FORM-08-GG-INF-02) o por medio de correo electrónico dirigido a helpdesk@ipsfa.com, ningún usuario podrá solicitar modificaciones a los aplicativos si no es por medio del responsable del mismo.

C. MENSAJERÍA Y CORREO ELECTRONICO

1.0 SOBRE EL SOFTWARE DE MENSAJERÍA

- 1.1 El Jefe de cada área organizativa del Instituto, será responsable del uso adecuado del software de mensajería, por parte del personal que se encuentre bajo su responsabilidad y velará porque dicha herramienta sea utilizada en beneficio de su trabajo.
- 1.2 Quedará al juicio del jefe de cada área organizativa del Instituto la suspensión del acceso a Internet.
- 1.3 Todo requerimiento de acceso a Internet deberá ser gestionado por el jefe de cada área organizativa del Instituto a través del formulario respectivo.



- 1.4 El Administrador de Red, deberá monitorear el ancho de banda de los servicios de Internet contratados para el mejor desempeño de este servicio.

2.0 PARA LA ASIGNACIÓN DE CUENTAS DE CORREO ELECTRÓNICO

- 2.1 Proteger su cuenta de usuario asignada: guardar el secreto de su password, no prestar su clave de usuario bajo ninguna circunstancia.
- 2.2 Responsabilizarse de cualquier actividad que se realice con su password.
- 2.3 Hacer los respaldos correspondientes a su información particular en su disco duro y/o cualquier medio magnético, así como borrar periódicamente sus correos y archivos.
- 2.4 En cuanto a los password, la Unidad de Informática, dependiendo de alguna amenaza, podrá forzar a cambiar su password a todos los usuarios, usar programas para fijar password no reusables y encriptación de password, etc.
- 2.5 Los usuarios internos y externos estarán obligados a cumplir con las normas y políticas dadas por la Unidad de Informática.

3.0 PARA USUARIOS INTERNOS DE CORREO ELECTRÓNICO

- 3.1 Todo empleado del IPSFA con un equipo asignado para su uso y que sea autorizado por su jefe inmediato superior tendrá acceso a una cuenta y correo electrónico en el servidor designado para tales efectos en la Unidad de Informática mientras sea empleado del Instituto.
- 3.2 Es responsabilidad del usuario hacer buen uso de su cuenta de correo electrónico, entendiendo por buen uso:
 - a. El no enviar ni contestar cadenas de correo electrónico.
 - b. El uso de su cuenta de correo electrónico con fines de trabajo
 - c. La depuración de su bandeja de entrada de correos (INBOX) del servidor (no dejar correos por largos períodos).
 - d. El no hacer uso de la cuenta para fines comerciales.
 - e. El respetar las cuentas de correo electrónico de otros usuarios Internos y Externos.
 - f. El uso de un lenguaje apropiado en sus comunicaciones.
- 3.3 El estándar establecido para la creación de cuentas de correo electrónico es:
nombre.apellido@ipsfa.com



- 3.4 Se asignará solamente una cuenta por usuario con su correo electrónico bajo el estándar establecido.
- 3.5 La creación de otras cuentas de correo electrónico se dará a consideración de la Unidad o Departamento solicitante.
- 3.6 La cuenta de correo es personal e intransferible no permitiéndose que segundas personas hagan uso de ella.
- 3.7 La vigencia de la cuenta de correo electrónico es durante la persona sea empleado del IPSFA.
- 3.8 El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS de información o anexos que pudieran contener información nociva para otro usuario como virus o pornografía.
- 3.9 El usuario es responsable de respaldar sus archivos de correo manteniendo en el buzón de correo (INBOX) solamente documentos adjuntos mas recientes, sus demás comunicados deberá mantenerlos en su equipo personal o en su defecto en la(s) carpeta(s) asignada(s) en el servidor para su área y/o Departamento.
- 3.10 Al responder comunicados generales o para un grupo específico de usuarios, el usuario deberá cuidar de no responder a TODOS los usuarios salvo cuando ésta sea la finalidad de la respuesta.
- 3.11 La Unidad de Informática se reserva el derecho de enviar al usuario la información que considere necesaria como un medio de comunicación Institucional.
- 3.12 La vigencia y espacio de las cuentas será definido por la Unidad de Informática de acuerdo a los recursos disponibles y con base en las necesidades del usuario.
- 3.13 La Unidad de Informática se reservará el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad Institucional.
- 3.14 La Unidad de Informática realizará monitoreo del tamaño de los buzones y deshabilitará aquellos que considere que estén afectando la disponibilidad de espacio del servidor.
- 3.15 El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.
- 3.16 El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y posterior baja del sistema de su cuenta.



- 3.17 El usuario podrá generar sus listas de distribución de correo con un máximo de 20 direcciones de correo, siempre y cuando éstas no interfieran con el buen funcionamiento y la distribución del correo del servidor.
- 3.18 La Unidad de Informática no se compromete a entregar mensajes de correo a cuentas de uso gratuito como hotmail, yahoo, usa.net, excite, starmedia etc.

4.0 PARA USUARIOS EXTERNOS DE CORREO ELECTRÓNICO

- 4.1 Las cuentas y correos electrónicos para usuarios externos serán solicitados por la UCEFI (cuando se trate de los entes fiscalizadores del IPSFA) y/o a través de la Gerencia del IPSFA que desee un servicio de este tipo, especificando el objetivo del servicio solicitado y el período por el cual se requiere.
- 4.2 Es responsabilidad de la UCEFI notificar de forma inmediata a la Unidad de Informática cuando el servicio solicitado para un usuario externo perteneciente a un ente fiscalizador ya no tenga validez.
- 4.3 La Unidad de Informática facilitará a los usuarios manejar el correo electrónico a través de sus cuentas, siendo éste un medio de comunicación formal a nivel Institucional, por lo que enviará los avisos y mensajes que considere necesarios a través de este medio.
- 4.4 Por seguridad (ya que en ellos puede disfrazarse un virus) no se pueden enviar, ni recibir archivos a través del correo electrónico institucional @ipsfa.com, aquellos que cumplan con los siguientes criterios y extensiones:

.ad.adb*.ade*.adp*.asp*.bas*.bat*.chm*.cmd*.com*.cpl*.crt*.dbx*.eml*.exe*.hlp*.hta*.htm*.html*.inf*.ins*.isp*.js*.jse*.lnk*.mde*.mdb*.mht*.mp3*.msc*.msi*.msp*.mst*.oft*.pcd*.pl*.pif*.php*.reg*.scr*.sct*.shb*.shs*.sht*.ttb*.txt*.uin*.rtf*.url*.vb*.vbe*.vbs*.vsd*.vss*.vst*.vsw*.wab*.ws*.wsc*.wsf*.wsh*.pif*.scr*.exe*.cmd*.bat*.zip*.emlbody.*.data.*.doc.*.document.*.file.*.message.*.readme.*.test.*.text.**.http.folder.htt*.msg
document.*
msg.*
doc.*
talk.*
massage.*
creditcard.*



details.*
attachment.*
me.*
stuff.*
posting.*
textfile.*
concert.*
information.*
note.*
bill.*
swimmingpool.*

D. FALTAS Y SANCIONES A LOS USUARIOS

1.0 FALTAS

- 1.1 Consumir alimentos, bebidas o fumar frente al equipo asignado.
- 1.2 Utilizar servicio de voz, sonido o imagen no autorizados.
- 1.3 Usar lenguaje soez en la comunicación de Internet y/o en correo electrónico.
- 1.4 Demorar la entrega de equipo en préstamo cuando sea solicitado por la Unidad de Informática, para labores de mantenimiento.
- 1.5 Conectar periféricos al equipo sin previa autorización por escrito a la jefatura de Informática.
- 1.6 Instalar juegos y jugar en las computadoras.
- 1.7 Utilizar Internet para fines no institucionales.
- 1.8 Consultar y/o desplegar cualquier tipo de erotismo o de pornografía.
- 1.9 Mover máquinas, equipos, cables u otros elementos, sin supervisión y/o autorización de la unidad de Informática.
- 1.10 Utilizar el equipo asignado para piratería o acceso no autorizado (hacking) a servidores propios o ajenos.
- 1.11 Borrar el Software instalado por la unidad de informática.
- 1.12 Irrespetar de palabra o acción a los técnicos de la unidad de informática.
- 1.13 Realizar acción voluntaria que cause daño a los equipos asignados.
- 1.14 Causar daños o perjuicios a terceras personas.



1.15 Otras, que afecten en forma grave el funcionamiento del equipo asignado o la red institucional.

1.16 Instalar software sin licencia, violando las leyes o regulaciones tales como la ley, reglamento de fomento y protección de la propiedad intelectual, en la instalación de software en el equipo asignado.

2.0 SANCIONES

2.1 Amonestación por escrito con copia al expediente la primera vez.

2.2 Amonestación por escrito y suspensión del uso del servicio por un período de 3 meses en el caso de los incisos c, e, f y g.

2.3 Las indicadas en los incisos i, k, l y m se sancionarán por primera vez con amonestación escrita y suspensión temporal del equipo y/o servicio asignado; las reincidencias darán lugar a la suspensión definitiva del equipo y/o servicio asignado.

2.4 Las restantes faltas, serán sancionadas con la suspensión definitiva del equipo y/o servicio asignado.

2.5 Las amonestaciones por escrito serán comunicadas por el área de RRHH del IPSFA a petición de la jefatura de la Unidad de Informática o de otra autoridad Institucional.

2.6 Las sanciones por faltas graves serán comunicadas por el área de RRHH.

2.7 El uso de software sin licencia, será responsabilidad directa del usuario el cual responderá ante los entes fiscalizadores.

E. RED INSTITUCIONAL

1.0 PARA EL USO DE LA RED INSTITUCIONAL

1.1 Los servicios disponibles son: correo electrónico, acceso a red institucional, acceso a los aplicativos institucionales, acceso a Internet y acceso a los directorios de red Institucional

1.2 Las Gerencias y Jefaturas solicitarán por escrito a la Unidad de Informática acceso para sus colaboradores a los servicios disponibles, con la respectiva justificación en el formulario para tal solicitud.



- 1.3 Los servicios son un privilegio, no un derecho, los mismos implican responsabilidad. Cualquier violación a las políticas establecidas puede resultar en la pérdida de los servicios y tomar acciones disciplinarias adicionales, las cuales podrán determinarse a nivel administrativo siguiendo los procedimientos existentes.
- 1.4 Cada usuario será responsable de las acciones efectuadas a través de los diferentes servicios que se le autoricen.
- 1.5 Los servicios ya otorgados y/o solicitados pueden ser negados al usuario que sea identificado como un riesgo de seguridad o tenga un historial problemático con otros accesos y/o sistemas computacionales a nivel Institucional.
- 1.6 La Unidad Informática tiene la responsabilidad de controlar y recomendar suspender el servicio a cualquier usuario que viole las políticas o interfiera con los derechos de otros usuarios.
- 1.7 La Unidad Informática tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.
- 1.8 El estándar establecido para la creación de usuarios de red Institucional y para acceso a los aplicativos del IPSFA (Contabilidad, Compras, etc) es: **primera letra del nombre+apellido**, ejemplo: **José Eduardo López Martínez** sería **jlopez**.
- 1.9 De existir un usuario previo con el mismo acceso, se utilizará la primera letra del segundo nombre o el segundo apellido en lugar del primero, según sea el caso, ejemplos:
 - a. José Eduardo López Martínez podría ser elopez
 - b. José Eduardo López Martínez podría ser jmartinez.
 - c. José Eduardo López Martínez podría ser emartinez.
 - d. **Etc.**

2.0 SEGURIDAD Y ACCESO EN LA RED INSTITUCIONAL.

- 2.1 El usuario puede cambiar su contraseña, de no cambiarla el servidor le avisa que debe hacerlo, sin intervención del administrador de red.
- 2.2 El acceso a la red es restringido, los usuarios solamente pueden hacer uso de las aplicaciones instaladas en el servidor y herramientas instaladas en su PC.
- 2.3 Los usuarios no están autorizados para instalar software en sus equipos asignados.
- 2.4 Para intercambiar información con otras Unidades tienen dos alternativas
- 2.5 Una carpeta Institucional (común a todas las áreas)



- 2.6 Enviar la información adjunta en el correo electrónico interno el IPSFA como máximo debe contener 10MB.
- 2.7 Las políticas de seguridad de la red, son administradas desde el servidor controlador del dominio, el cual tiene diferentes tipos de usuarios que por medio de él acceden a la red, los cuales son:
- Administrador:** Este usuario tiene todos los derechos para la administración de los servidores y monitoreo de usuarios de red.
- Usuario de Operador Informático:** Tiene la capacidad de realizar algunas configuraciones a los equipos instalados en la red, respaldo de los servidores.
- Usuario de Red:** estos usuarios tienen derecho de acceder a la red pero no puede realizar cambios en los equipos, se han tomado medidas de seguridad las cuales se pueden nombrar las siguientes:
- El usuario puede cambiar su contraseña, de no cambiarla el servidor le avisa que debe hacerlo, en un periodo basado en los estándares de un controlador de dominio sin intervención del administrador de red y de esta forma es personalizado.
 - El acceso a la red es restringido, los usuarios solamente pueden hacer uso de las aplicaciones instaladas en el servidor y herramientas instaladas en su PC.
 - El usuario no puede cambiar el entorno de su PC.
 - No puede instalar programas sin previa autorización.
 - El usuario no puede tener acceso al panel de control de sus equipos.
 - No puede ejecutar y cambiar la configuración de la red.
 - No tiene acceso al registro del sistema.
 - No puede editar desde la consola de Comandos.
 - Todos los equipos (pc's y laptop's) deben tener instalado un antivirus corporativo, que es administrado desde un servidor.
- 2.8 Las medidas de seguridad que se han tomado, son para que el usuario no cambie el ambiente de su PC ocasionando fallas o que instale programas no autorizados y que no sean requeridos para el desarrollo de sus labores.
- 2.9 Dentro de la Red cada Unidad o Departamento tiene acceso a una carpeta compartida; solamente colaboradores del Departamento tiene acceso a ella; con el objetivo de intercambiarse información.



F. INTERNET

4.0 ACCESO AL INTERNET.

- 4.1 Las Jefaturas son responsables de solicitar a la unidad de Informática el acceso de aquellos subalternos que para fines de trabajo tendrán acceso a Internet.
- 4.2 La solicitud será hecha por escrito en el formulario correspondiente.
- 4.3 El uso de Internet es exclusivamente para las actividades Institucionales.
- 4.4 Las configuraciones de las estaciones de trabajo para acceder al servicio de Internet son responsabilidad exclusiva del personal de la Unidad Informática.
- 4.5 El uso de Internet es personal e intransferible, no se permite que segundas personas (personas externas al IPSFA) hagan uso del servicio.
- 4.6 Se harán excepciones para el uso de Internet cuando este sea requerido, justificado y autorizado para los integrantes de las delegaciones de los entes fiscalizadores con presencia en el Instituto.
- 4.7 A través de los equipos de monitoreo y análisis de tráfico instalados en el sitio central de la red, se detectarán a los usuarios que hagan mal uso de los servicios de Internet.
- 4.8 Las Gerencias y Jefaturas solicitarán, si así lo consideran conveniente, que se limite el acceso para determinados usuarios a sitios específicos de Internet.
- 4.9 El Departamento de Recursos Humanos deberá informar a la Unidad de Informática inmediatamente cuando un empleado ha dejado de laborar en el IPSFA, con el objetivo de inhabilitar su acceso a Internet, correo electrónico, etc.

5.0 SEGURIDAD EN INTERNET

- 5.1 Todo archivo que se reciba por Internet es analizado automáticamente por el antivirus corporativo para asegurar que no contenga virus
- 5.2 Antes de abrir cualquier archivo recibido por Internet, el usuario debe asegurarse de que sea un archivo confiable.
- 5.3 El incumplimiento de la Normatividad Técnica en Tecnología de la Información, específicamente en el uso de Internet, será sancionado en los términos que establece la Ley de Responsabilidades Administrativas de los servidores Públicos.



I. MISCELANEOS

A. DISPOSICIONES FINALES

1. Las presentes Políticas entrarán en vigencia a partir de la fecha de su aprobación.
2. Toda modificación, deberá ser canalizada a través de la Unidad de Desarrollo Organizacional y deberá quedar debidamente documentada.
3. La aprobación de cualquier cambio a los procesos de trabajo establecidos, será responsabilidad exclusiva del Jefe de la Unidad o Gerente de Área respectiva.

B. ANEXOS

1. Solicitud y Análisis de Requerimientos. (FORM-08-GG-INF-01).
2. Solicitud de Acceso a Internet y Software de Mensajería. (FORM-08-GG-INF-02).

