| Sección | Emitido por: | Efectivo en: |
|---|---|---|
| **Normas sobre el Uso de los Sistemas Electrónicos de la OPPEA** | Carmen D. Sánchez Salgado, Ph. D.<br>Procuradora | 1 de agosto de 2001<br>Revisado 8/4/2014 |

## Propósito

El propósito de este Manual es establecer las guías, políticas y procedimientos para la Administración y Operación de la Red de Computadoras de la Oficina del Procurador de las Personas de Edad Avanzada. El personal o encargado de la Red de la OPPEA deben utilizar los Procedimientos Operacionales descritos en este Manual para proveer servicios en las siguientes áreas de la Red:

- Operación.
- Apoyo y mantenimiento
- Administración y monitoreo
- Auditoría del uso y la ejecutoria

1. Las guías de trabajo y los procedimientos aseguran que los servicios provistos sean efectuados y completados en una forma controlada y estándar.
2. Los parámetros establecidos aseguran la administración adecuada de la Red.
3. Los procedimientos operacionales permiten la continuidad de los procesos de surgir situaciones de emergencia y en caso de ausencia de personal clave.
4. Las políticas establecen el uso apropiado y correcto de los sistemas de información y activos de la Agencia que debe seguir todo el personal que labora en la misma.

## Alcance

Este documento aplica a toda la red de computadoras personales, la cual incluye los equipos de computadoras, equipos periféricos, sistemas operativos y aplicaciones así como al personal responsable por la operación y uso de la Red (personal de sistemas de información y usuarios).

## Definiciones

Los siguientes conceptos técnicos son usados con frecuencia en el contenido de este Manual. A continuación sus definiciones para referencia de los usuarios del mismo:

1. **AD (Active Directory):** Introducido en **Windows 2003**, es la base de la Red distribuida de **Windows 2003**. Facilita el uso de técnicas centralizadas y descentralizadas de manejo del dominio, incluyendo **Group Policies y Remote Administration**.
2. **Cable de la Red / *Network Cabling*:** Medio de transmisión utilizados para el transporte de datos dentro de una Red de ordenadores. Los tipos de cables más utilizados son:
   a. **Cable de Pares con Cubierta/*Shielded Twisted Pair (STP)*:** Cable trenzado que utiliza una cubierta de tejido de cobre, una envoltura de aluminio entre y alrededor de las parejas de cables y una torcedura interna en las parejas de cables para protegerlos aún más de cualquier ruido eléctrico producido por fuentes externas. Es un cable sumamente grueso que se usa mayormente en Redes Token-Ring.
   b. **Cable de Fibra Óptica / *Optic Fiber Cable*:** Utilizado para la transmisión de información mediante pulsos de luz, donde se requiere una fuente de luz, un detector y el cable que es el medio transmisor compuesto de una fibra ultra delgada de vidrio llamada núcleo, recubierto por un revestimiento exterior con índice de refracción menor que el del núcleo. Proporcionan un ancho de banda extremadamente grande, tienen una pérdida de potencia muy pequeña, no se afecta por alteraciones de voltaje o de corriente en las líneas, por interferencia electromagnética o por químicos corrosivos dispersos en el aire y es un cable mucho más delgado que los anteriores.
   c. **Cables de Pares Sencillo /*Unshielded Twisted Pair (UTP wire)*:** Está formado por dos hilos de cobre aislados y torcidos entre sí formando algo parecido a la trenza para Reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor. El cable resultante está cubierto por una capa aislante externa.
   d. **Cables de 4 Pares Categoría 5E "Plenum" / *Plenum Cable Cat.5E*:** Cable que está formado por 4 pares de hilos de cobre aislados. A su vez está cubierto por una capa externa que está aprobada por el Código Nacional Eléctrico para el uso en espacios abiertos. Esta capa es resistente al fuego.

3. **Cliente o estación de usuario / *Workstation*:** la computadora que utiliza el usuario para tener acceso a la Red.
4. **Concentrador / *Hub*: componente** de conectividad que provee una conexión común entre las computadoras en una Red de estrella.
5. **DHCP (Dynamic Host Configuration Control Protocol):** Servicio en el cual Windows 2012 asigna los IP a las estaciones, y guarda los parámetros del esquema de IP de la Red en su base de datos.
6. **Dirección / *Network Address*–** en toda Red se le asigna a cada dispositivo o nodo capaz de comunicarse, una dirección de nodo o código único que los demás pueden emplear cuando le transmiten información.
   a. La dirección de nodo depende del protocolo que se emplee.
   b. Cada protocolo emplea su propio esquema para las direcciones.
   c. En algunos casos, un mismo nodo puede funcionar con más de un protocolo y tener una dirección distinta para cada uno de ellos.
   d. Los protocolos se usan también para asignar direcciones a las propias Redes, conocida como dirección de la Red, que suele formar parte de la dirección de cada Red, de forma tal que al emplearla, se sabe también a la Red que pertenece.
7. **Dispositivos de Conexión / *Network Devices*:** son tarjetas de Red, cables o cualquier medio físico que permita a los ordenadores intercambiar bytes de información y otros equipos, como puede ser un *HUB* o un Switch Box, necesarios para conectar los ordenadores entre sí, de modo que quede formada la Red local. Las grandes empresas suelen hacer uso de otras Redes de comunicaciones, como puede ser la Red telefónica, para interconectar sus Redes locales entre sí.
8. **Dispositivos de Respaldo / *Resguardo (backup)Devices*:** unidades periféricas que, conectadas a la Red, se utilizan para respaldar o copiar la información almacenada en los servidores, como medida de prevención en caso que sea necesaria su recuperación.
9. **DNS (Domain Name System):** Requerido para la operación de **Active Directory**, es el servicio en **Windows 2012** que traduce de un nombre a un objeto o información y su lugar en **Active Directory**.
10. **Dominio / *Domain*:** agrupación lógica de las computadoras que comparten la misma base de datos de las cuentas, grupos de usuarios, recursos y políticas de seguridad. Para cada dominio existe un nombre único.

11. **Enrutador / *Router*:** Un dispositivo que conecta las Redes de diversos tipos, como las que usan diferentes arquitecturas y protocolos. Los enrutadores determinan el mejor camino para enviar datos y filtran el tráfico de la difusión al segmento local.
12. **GPO (Group Policy Object.):** Colección de restricciones y políticas a aplicarse a las computadoras o usuarios que están dentro de los OU.
13. **Group Policies:** Introducido en **Windows 2000**, permite la implementación de estándares y políticas de la agencia a la Red de computadoras
14. **Métodos de Acceso en la Red: s**e refiere a los convencionalismos de comunicación utilizados por las computadoras para comunicarse entre sí en una Red. Es algo así como el lenguaje (español, inglés). Los tipos de métodos más usados son:
    a. **Arcnet:** Es una Red en banda base que transmite a una velocidad de 2.5 Mbps, con una topología híbrida estrella/bus. Este sistema fue desarrollado en 1978 por la empresa Datapoint, aunque fue potenciado en el mundo de los microordenadores por la empresa Standard Microsystems. Todos los ordenadores de la Red se conectan en estrella a un distribuidor central denominado HUB activo.
    b. **Token Ring**: Es una Red en anillo con paso de una llave o testigo. Eso significa que los ordenadores conectados a la Red se van pasando un testigo de unas a otras de forma secuencial y cíclica, de modo que sólo puede transmitir información aquel ordenador que posea el testigo en un momento dado. Como la velocidad de transmisión de este tipo de Redes puede ser hasta 16 Mbps, el usuario no se da cuenta del tiempo que tiene que esperar su ordenador antes de recibir el nuevo testigo para poder empezar a transmitir.
    c. **Ethernet:** Ethernet emplea una topología en bus con el método CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) para acceder al medio, que sigue el estándar IEEE 802.3. Eso significa que cualquier estación puede intentar transmitir datos en cualquier momento, pero como todas ellas están conectadas a un único cable común, solo una estación puede estar transmitiendo por el cable (bus) en un momento dado. Para solucionar los problemas de colisiones en la transmisión existen una serie de normas como son: antes de transmitir comprobar que no haya otra estación transmitiendo, o que en caso de colisión hacer que una estación espere un margen de tiempo aleatorio antes de volver a intentar el envío de datos. Todas estas tareas son realizadas automáticamente por el software de Red a unas velocidades tan elevadas que el usuario no se da cuenta de las colisiones.

15. **MMC (Microsoft Management Console.):** Introducida en **Windows 2003**, es la herramienta básica para centralizar el manejo de AD y sus componentes, como **Group Policies.**

16. **Modulador-DeModulador / *Modem*:** Es un periférico que permite que dos ordenadores se puedan comunicar entre sí vía Red telefónica conmutada. En este caso, uno de esos ordenadores formará parte de la Red, mientras que el otro será remoto.

17. **OU (Organizational Unit):** Es un "*objeto*" situado en el **Active Directory**, al cual se le aplican los **Group Policies**. Estos objetos pueden ser un contenedor que incluya usuarios o computadoras.

18. **Policy**. Consiste en un grupo de configuraciones de registry que define los recursos de la Red o computadora disponible para un usuario o grupo.

19. **Portales / *Gateways*:** Es un hardware y software que permite las comunicaciones entre la Red local y grandes ordenadores (*mainframes*). El *gateway* adapta los protocolos de comunicación del *mainframe* (X25, SNA, etc.) a los de la Red, y viceversa.

20. **Protocolo de la Red / *Network Protocol*:** acuerdo estandarizado que establece la forma en que las transmisiones tendrán lugar a través de la Red. Son conjuntos de normas que definen los múltiples aspectos que intervienen en una comunicación como iniciar, terminar, secuencia de mensajes a emplear e identificación de interlocutores.

    a. La mayoría de la información en una Red viaja en **paquetes**.

    b. Los protocolos definen desde el formato que han de tener los paquetes hasta las órdenes que un dispositivo puede aceptar.

    c. La Red tiene un único conjunto de protocolos para su operación.

    d. Principales Protocolos Utilizados:

        1) **NetBios**–protocolos definidos por IBM y Microsoft para Redes de área de local o metropolitana.

        2) **TCP/IP**–"Transmission Control Protocol/Internet Protocol", son los protocolos desarrollados por el Departamento de la Defensa de los Estados Unidos para su Red de conmutación de paquetes ARPA. Este es el protocolo utilizado en el Internet y es de las Redes en máquinas **UNIX.**

3) **IPX/SPX**–"Internet Packet exchange/Sequential Packet exchange", son protocolos definidos por la compañía Novell como soporte de sus Redes de área local.

4) **Apple Talk**–protocolos desarrollados por la compañía Apple para Redes de ordenadores Apple.

21. **Puentes / *Bridges*:** Es un hardware y software que permiten que se conecten dos Redes locales entre sí. Un puente interno es el que se instala en un servidor de la Red, y un puente externo es el que se hace sobre una estación de trabajo de la misma Red. Generalmente, se usa un puente externo con una estación dedicada para incrementar de esa forma el rendimiento de la interconexión. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a Redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan Redes distintas entre sí, llevando a cabo la conexión a través de Redes públicas, como la Red telefónica, RDSI o Red de conmutación de paquetes.

22. **RAID -** (arsenal de discos Redundantes) **/ *Redundad Array of Inexpensive Disks*:** Una estandarización de las opciones de la tolerancia de incidente en cinco niveles. Los niveles ofrecen varias combinaciones del funcionamiento, de la confiabilidad y de los costos, mediante la combinación en el uso de varios discos fijos en el almacenamiento de los datos. **Windows NT** sólo la trabaja con los niveles 0, 1 y 5.

23. **RAID - Niveles**

a. Raid 0 – se reparte la información entre los discos configurados para esta opción pero no existe redundancia entre ellos.

b. Raid 1 - también se conoce como *mirroring*, requiere dos discos para duplicar la información de las particiones en ambos discos a la vez.

c. Raid 2, 3 y 4– son modos donde se reparte la información entre los discos disponibles con código de corrección de error, con paridad y/o en bloques de información más grandes. (no aplican en **Windows NT**)

d. Raid 5 - se reparte la información entre los discos disponibles estableciendo un nivel mayor de Redundancia. La data y el bloque de paridad se almacenan en los discos de forma alternada para que nunca estén en el mismo disco. Se requiere un mínimo de tres discos para lograr esta redundancia.

e. **Red / *Network***: Conjunto de ordenadores o computadoras conectadas entre sí que nos permite compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia software) y periféricos como puede ser

un módem, una tarjeta RDSI, una impresora, un escáner, etc. Las redes locales *(Local Area Network),* permiten interconectar ordenadores que estén dentro de un mismo edificio o en edificios colindantes, pero siempre teniendo en cuenta que el medio físico que los une no puede tener más de unos miles de metros. Para unir ordenadores separados por grandes distancias se hace uso de las redes de área extensa (*WAN, Wide Area Network*), las cuales se sirven de otras redes de comunicaciones como puede ser la red telefónica para transmitir información entre los ordenadores comunicantes.

24. **SCSI**- interfaz pequeño del sistema informático*)/(**Small Computer System Interface)*:** Una interfaz paralela estándar de alta velocidad, definida por el ANSI. Se utiliza para conectar los microordenadores con los dispositivos periféricos, tales como discos duros e impresoras y con los otros ordenadores y LANs.

25. **Servidores / *Servers*:** Aquel o aquellos ordenadores o computadoras que van a compartir sus recursos hardware y software con los demás equipos de la Red. Son responsables de controlar la operación de la Red y del manejo de los recursos disponibles en la misma. Se conoce como servidores de archivos o *file servers* a los servidores donde se almacenan los distintos archivos de los usuarios, programas o bases de datos. Los servidores de comunicaciones manejan los programas que establecen el tráfico de comunicación entre las computadoras de Red, mediante los equipos de comunicación.

26. **Sistema Operativo de la Red / *Network Operating System (NOS)*:** familia de programas que permiten a las computadoras de la Red el intercambio de información, el uso compartido de recursos y el manejo de todas las operaciones de comunicaciones en la Red. El usuario en ningún momento tiene conocimiento de si la información a la cual está accediendo se encuentra en su propio ordenador o en otro distinto dentro de su Red local o en cualquier otra parte del mundo.

27. **Tarjeta de Conexión a la Red / *Network Adapter Card (LAN adapter)*:** Tarjeta de expansión que se instala en las computadoras de usuario para lograr la conexión con el servidor de la Red. Es responsable por cambiar la señal interna de la computadora en una señal de mayor potencia, capaz de viajar por el cable de la Red.

28. **Topología de Redes / *Network Topology*:** La topología de una Red de ordenadores hace referencia a como se distribuye u organiza el conjunto de ordenadores dentro de la Red, en lo que al diseño del cableado respecta. Entre las más conocidas están:

a. **Topología en Anillo /*Ring Network*:** Todas las estaciones están conectadas entre sí formando un anillo, de modo que cada estación tiene conexión directa con otras dos. Los datos viajan por el anillo de estación en estación siguiendo una única dirección, de manera que todas las informaciones pasan por todas las estaciones hasta llegar a la estación de destino, en donde se quedan. Cada estación se queda con la información que va dirigida a ella y retransmite al nodo siguiente las que tienen otra dirección.

b. **Topología en Bus / *Bus Network:*** Todas las estaciones están conectadas a un único canal de comunicaciones, toda la información circula por ese canal y cada estación se queda solamente con la información que va dirigida a ella.

c. **Topología en Estrella / *Star Network:*** La topología en estrella es una de las más antiguas, en ella, todas las estaciones están conectadas a un ordenador central que actúa a modo de servidor. Todas las comunicaciones entre las estaciones se realizan a través del ordenador central, que es el que controla la prioridad, procedencia y distribución de los mensajes. El ordenador central será normalmente el servidor de la Red, aunque puede ser un dispositivo especial de conexión.

d. **Topología combinada Estrella-Bus / *Star Bus Network:*** En la topología estrella/bus, un multiplexor de señal ocupa la posición del dispositivo central de la Red en estrella, estando determinados ordenadores conectados en estrella al multiplexor y otros ordenadores, junto con los multiplexores conectados a un mismo bus.

## Responsabilidades

Algunas responsabilidades del personal, con respecto a la Red de OPPEA, se resumen a continuación:

1. Los técnicos de la Red de computadora son responsables de operar el sistema de acuerdo a los procedimientos establecidos.
    a. Ejecutar procesos de actualización de sistema.
    b. Generar reportes.
    c. Efectuar resguardos (*backups*).

d. Asegurar el acceso a las aplicaciones de la Red que están disponibles a los usuarios correspondientes.
e. Asegurar que la Red está en condición operacional.
f. Asegurar que los usuarios tienen el abastecimiento necesario para proceder con las operaciones corrientes.
g. Notificar cualquier situación para el acuerdo debido.
h. Mantener un registro claro de actividades operacionales.
i. Prestar apoyo en la soluciones de problemas a los usuarios de la Red.

2. El Administrador de la Red o su designado es responsable de:
   a. Asegurar el cumplimiento de todos los procedimientos establecidos en este manual.
   b. Supervisar el personal técnico de la Red.
   c. Revisar los programas de trabajo del sistema.
   d. Asegurar la continuación de operación del sistema y que se completen los trabajos diarios.
   e. Hacer cumplir los procedimientos estándares diarios.
   f. Asignar requerimientos especiales de proceso de data.
   g. Mantener el equipo y facilidades relacionadas en condiciones óptimas.
   h. Administrar el establecimiento de seguridad de la Red.
   i. Monitorear el rendimiento de la Red.
   j. Administrar sistema de inventario de data.
   k. Monitorear el rendimiento de las aplicaciones anti-virus.
   l. Instalar y dar apoyo a los programas de computadoras personales.
   m. Investigar sobre software de oficina y network.
   n. Administrar servidores.

3. Director o su designado es responsable de:

   a. Administrar y controlar todas las fases funcionales del sistema de información incluyendo base de datos, computador central, software, recursos humanos y las actividades de la Oficina de Sistemas de Información de la Agencia bajo la dirección del supervisor inmediato.

   b. Administrar el tiempo, la utilización e inventario de todo equipo electrónico y del procesamiento de datos para las operaciones.

   c. Recomendar e implementar medidas de seguridad, planes de contingencia, planos de reanudación de negocio para protección de los recursos de computadoras, sistemas de información y facilidades de centro de data.

   d. Facilitar, apoyar y adaptar una estrategia de negocio en conformidad con las metas, planificación y controles de la Agencia.

   e. Asegurar que se han establecido procedimientos, planos y controles necesarios para operar la Red de computadora para exitosamente completar los requisitos de proceso de data, flujo de información y servicio de apoyo requerido para los usuarios.

   f. Asegurar que el personal bajo su supervisión conozca y cumpla con las Políticas establecidas.

---

**Introducción :**

La Oficina Del Procurador de las Personas de Edad Avanzada (OPPEA) cuenta con acceso a computadoras, redes, servicios electrónicos internos y a la red Internet. De la única forma en que usted puede utilizar esta computadora y los servicios asociados es entendiendo y aceptando las siguientes condiciones:

**Titularidad y Derechos**

- Esta computadora, los servicios asociados tanto internos como externos, el sistema de correspondencia electrónica (e-mail), la Intranet, el acceso a la Internet y los documentos y programas que existen en la misma, son propiedad de la OPPEA y sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de esta Oficina.

- Toda información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de una de las computadoras de la OPPEA, será

propiedad de la Oficina, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.

- La información contenida en esta computadora, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (e-mails), información de la Intranet o la Internet y los documentos y programas existentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes de la OPPEA.

- Se prohíbe terminantemente utilizar programas o recursos para los cuales no exista una licencia o autorización de uso válida a nombre de la OPPEA.

- Se prohíbe terminantemente copiar programas de la OPPEA para instalarlos en otras computadoras, sin la autorización por escrito de la Procuradora.

- Se prohíbe terminantemente el instalar programas en las computadoras de la OPPEA sin la autorización por escrito de la Procuradora.

- Se prohíbe el uso de los sistemas de computadoras y comunicaciones de la OPPEA para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes en cadena. De igual forma, el usuario no podrá utilizar los recursos electrónicos de la OPPEA para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones de la OPPEA.

- Se prohíbe acceder a, o utilizar propiedad intelectual ("copyrighted information") que viole los derechos de autor.

Seguridad

- El uso de un código de acceso ("password"), no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquier otra. Las contraseñas deben mantenerse en estricta confidencialidad y administrarse conforme al Memorando sobre medidas de seguridad adoptadas por la OPPEA. Al aceptar utilizar esta computadora usted reconoce haber leído y entendido dicho Memorando.

- La OPPEA se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad se utilice para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente o al azar, o cuando exista una investigación sobre una situación en particular. Por estas circunstancias, el personal de la OPPEA no tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de "e-mail".

- Para evitar poner en peligro la confidencialidad de la información de la OPPEA, se prohíbe el envío fuera de la Oficina de documentos electrónicos o mensajes por medio del "e-mail" que contengan información confidencial.

- Se prohíbe el envío o recibo de mensajes de correo electrónico o de cualquier tipo entre el personal de la OPPEA y otras personas que no pertenezcan a la misma, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno de la OPPEA, que puedan poner en entredicho la reputación o imagen de la OPPEA, aunque la información divulgada no sea de naturaleza confidencial.

- Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.

- Se prohíbe codificar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos propiedad de la OPPEA con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos, o con el propósito de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar la información, mensajes o archivo, si no se obtiene previamente el consentimiento por escrito de la Procurador. En el caso de que por razones de seguridad se permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerla, la OPPEA estará facultada para decodificar la misma o restituirla a su condición original, y el usuario será responsable de proveer todos los datos para lograr acceso a la información o archivo.

- Se prohíbe la modificación de los parámetros o configuración de las computadoras de la OPPEA para darle la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de

la OPPEA.

- Se prohíbe el uso de discos magnéticos o cualquier otro medio de almacenaje de información, sin que haya sido verificado o certificado como libre de virus. Para ello se debe seguir el procedimiento de seguridad previamente establecido.

- Todos los archivos que se creen en las computadoras deben guardarse en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de resguardo (backup) existentes.

- Los usuarios deberán ser automáticamente forzados a cambiar su contraseña periódicamente y un formulario aprobado de mantenimiento de cuenta debe ser sometido al Administrador del Sistema de manera que se solicite cualquier cambio al expediente del usuario.

- Todo el personal con acceso a información computarizada que sea transferido de departamento u oficina o terminado su empleo, sus privilegios de acceso deberán ser terminados el mismo día que termine, sea transferido o promovido.

- Acceso a los sistemas de información del Departamento deberá ser requerido sometiendo un formulario debidamente aprobado de mantenimiento de cuenta del usuario. Cada usuario del sistema de información tendrá una combinación de cuenta/contraseña para acceder los sistemas. Las contraseñas de usuario se utilizarán solamente para el uso del individuo al que se les emitió. El usuario es responsable de proteger su cuenta/contraseña y de cada actividad registrada en el sistema bajo su cuenta.

- Todo el personal es responsable de cumplir con los estándares, políticas, procedimientos y controles establecidos para mantener un ambiente seguro. La Oficina de Sistemas de Información o representante de Seguridad es responsable de monitorear la ejecución de estos requisitos de seguridad.

- El personal deberá devolver la propiedad de la Agencia al cesar sus funciones. El personal es responsable por el uso apropiado y el cuidado de la propiedad que reciban y se comprometen a devolverla cuando terminen su trabajo con la Agencia. Este compromiso es formalizado al firmar el formulario de relevo.

- Los usuarios deben proteger su acceso desactivándose cada vez que dejan su estación de trabajo como manera de prevenir la divulgación no autorizada del

sistema. Cualquier computadora o terminal que se deje sin atender por más de diez (10) minutos, será automáticamente desactivado. El usuario será responsable de cualquier estación que se deje activa y desatendida.

- La posesión y uso de herramientas especializadas para romper los controles de seguridad en cualquier sistema, no será permitido en el Oficina del Procurador de las Personas de Edad Avanzada. Cualquier violación a esta política será penalizada aplicando el Reglamento de Conducta.

- El acceso remoto a los sistemas de información de la Agencia, deben ser solicitados y autorizados por el Procurador y el Director de Oficina de Sistemas de Información. El acceso será concedido solamente cuando las funciones de sus tareas requieran dicho acceso.

- El usuario necesita la autorización del Director al cual se reporta para utilizar el Internet o Intranet. El personal de la Agencia con líneas de acceso al Internet/Intranet deben utilizar dichas tecnologías para propósitos de trabajo solamente. El acceso es limitado para prevenir varios problemas tales como, bajar pornografía o cualquier otra práctica no deseada.

- El correo electrónico deberá ser utilizado para propósitos de trabajo solamente. Los mensajes del correo electrónico pertenecen a la Agencia por lo que se reserva el derecho de acceder y divulgar, para cualquier propósito, todos los mensajes enviados a través de los sistemas de la misma.

- Para erradicar los virus, se requiere el apoyo de la Oficina de Sistemas de Información y los usuarios no deberán erradicar los virus ellos mismos. Los usuarios no están autorizados a instalar ningún tipo de software en sus computadoras.

Políticas Operacionales Centro de Cómputos

- Acceso físico al área del Centro de Cómputos está restringida a personal autorizado solamente. Visitantes, incluyendo personal de otras áreas del Departamento, clientes y terceros, serán escoltados en todo momento por personal de la Oficina de Sistemas de Información y deberán firmar la entrada y salida en el Registro de Visitantes.

- Cada Oficina es responsable de mantener o suplir la impresora en su sección u oficina, de manera que puedan recibir los informes producidos y los cuales son

dirigidos a estas impresoras. También, los usuarios son responsables de recibir, revisar e informar cualquier situación que ocurra con los informes distribuidos mediante el sistema de correo interno de la Agencia.

Políticas de Hardware

- Equipo del centro de computadoras que sea de información, deberá mantenerse en áreas controladas y todo usuario será responsable de proteger y asegurar su equipo de sistemas de información.
- Equipo o software relacionado a computadoras deberá ser instalado y configurado por el personal de la Oficina de Sistemas de Información y solamente el equipo que cumpla con los estándares establecidos por la Agencia podrá ser adquirido.
- La adquisición de equipo nuevo o software o el reemplazo del existente se hará en base a la necesidad. Las solicitudes deberán someterse con la justificación apropiada y la Oficina de Sistemas de Información evaluará y determinará la necesidad.
- Todo usuario es responsable por el inventario de equipo y software de computadora o relacionado asignado a él/ella. Por dicha razón, él/ella deberá firmar el formulario de inventario correspondiente.
- No está permitido que ningún usuario comience el proceso de corregir los problemas ("troubleshooting") sin informarlo a la Oficina de Sistemas de Información, y bajo ninguna circunstancia están autorizados a instalar o utilizar una herramienta de diagnóstico personal en las computadoras de la Agencia.

Políticas de Auditorias

- Todo el personal es responsable de cooperar con los auditores durante las auditorias a la Oficina de Sistemas de Información efectuadas por personal del Departamento de Auditoria Interna.
- Todo el personal tiene la responsabilidad de estar consciente de los requisitos legales de los sistemas de información de la Agencia y el cumplimiento con las regulaciones aplicables. La Oficina del Contralor puede examinar periódicamente los sistemas en cuanto a los procedimientos de seguridad y validez.

## Políticas Antidiscrimen

- Existe una prohibición absoluta y cero tolerancias a la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, género, credo, ideas políticas u origen social o nacional, o que puedan ser catalogados como hostigamiento sexual.

- Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica de la OPPEA. Esto incluye a modo de ejemplo, acceso a materiales eróticos, bromas de cualquier forma o cualquier comentario o chiste que pueda violar la política de discrimen de la OPPEA o su política de hostigamiento sexual.

- Se prohíbe que se utilicen protectores de monitores (screen savers) con fotos de personas, artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que pueda resultar poco seria u ofensiva.

- Se prohíbe la divulgación por cualquier medio de cualquier tipo de opiniones personales específicas con relación a raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimento físico o mental.

## Correo Electrónico

- Se prohíbe que los usuarios utilicen durante horas laborables cuentas de correo electrónico distintas a las cuentas oficiales provistas por la OPPEA Ej: Correos Personales.

- Se prohíbe el envío a otras personas de copia de un mensaje de correspondencia electrónica recibido sin el conocimiento o consentimiento del remitente original.

- Se prohíbe leer, revisar o interceptar cualquier tipo de comunicación electrónica de la OPPEA o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.

- Se prohíbe que los usuarios se suscriban a listas de correo electrónico o que participen en grupos de noticias (newsgroups) que divulguen información o mensajes ajenos a las funciones y deberes de la OPPEA.

- No se podrá crear archivos o enviarlos mediante el correo electrónico que excedan la capacidad de la cuota del usuario en el servidor.

- Se prohíbe el envío de mensajes electrónicos alusivos a Religión, Material Pornográfico, Erótico, Político o Cualquiera otro asunto que pueda resultar ofensivo.

**Disposiciones Misceláneas**

- Se prohíbe el uso de programas de charlas (Chats) a menos que sean autorizados expresamente por la Procuradora.

- Las políticas antes mencionadas sobre el uso del correo electrónico y sus auditorías serán de igual aplicación para los otros recursos de la Intranet e Internet tales como el WWW, FTP, Chat, etc.

- Es responsabilidad de los usuarios el cumplir con las normas de cuotas de espacio en los servidores.

- Las políticas de Internet serán revisadas periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la OPPEA. Se incorporan y se hacen formar parte de estas advertencias todos los Documentos, Memorandos, Instrucciones, Manuales o Políticas que se notifiquen de tiempo en tiempo y que sean pertinentes al uso de las computadoras en la OPPEA.

**Aceptación y procedimientos disciplinarios**

- Se tomarán las medidas disciplinarias, civiles o criminales que correspondan contra los usuarios que violen estas políticas o abusen del acceso a la Internet, según sea el caso. En el caso de las medidas disciplinarias estas serán de acuerdo al Reglamento de Conducta establecido en la Agencia.

- La OPPEA se reserva el derecho de radicar acusaciones criminales por las actuaciones que constituyan delito federal o estatal aunque no estén expresamente prohibidas por estas condiciones de uso de los equipos de computadoras.

- Entiendo las normas citadas y acepto que se ha divulgado toda la información relacionada al uso de esta computadora. Además, el personal cualificado de la OPPEA está disponible para aclarar las dudas que me surjan en cuanto al cumplimiento de estas condiciones de uso.

- Acepto que es mi obligación conocer y seguir todas las políticas o instrucciones de la OPPEA en cuanto a las medidas de seguridad del uso del equipo de computadoras y de las redes disponibles, particularmente las *Normas adoptadas para la utilización del Internet.*

- El hecho de que una conducta o actuación relacionada con las computadoras, redes, sistemas y recursos electrónicos de la OPPEA no esté contemplada en estas advertencias y condiciones de uso de las computadoras, no impide que el usuario pueda ser sancionado, si a juicio de la Procuradora se trata de una conducta o actuación imprudente o irresponsable en relación a los referidos equipos y recursos electrónicos. A los fines de estas advertencias y condiciones de uso, una conducta o actuación imprudente o irresponsable significa cualquier acción directa o indirecta que ponga en riesgo la seguridad, integridad y confiabilidad de los equipos, las redes, la información, los programas y los sistemas de la OPPEA. Uso imprudente o irresponsable significa además, cualquier actuación o conducta directa o indirecta que pueda ocasionar daño físico, mental, moral, problemas interpersonales o un menoscabo de la reputación de los usuarios, personas ajenas a la OPPEA, la Procuradora o la Oficina de la Procuradora de las Personas de Edad Avanzada.

- Acepto además, que es mi obligación comunicar a la Procuradora o a la persona delegada a esos fines, cualquier situación, incidente o problema de seguridad, acceso indebido o violación voluntaria o involuntaria de estas normas, que surja en el uso de las computadoras o redes de la OPPEA.

Firma_____ Fecha_____

- La OPPEA se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad se utilice para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente o al azar, o cuando exista una investigación sobre una situación en particular. Por estas circunstancias, el personal de la OPPEA no tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de "e-mail".

- Para evitar poner en peligro la confidencialidad de la información de la OPPEA, se prohíbe el envío fuera de la Oficina de documentos electrónicos o mensajes por medio del "e-mail" que contengan información confidencial, salvo que estén autorizados por el supervisor o se relacione con las tareas asignadas.

- Se prohíbe el envío o recibo de mensajes de correo electrónico o de cualquier tipo entre el personal de la OPPEA y otras personas que no pertenezcan a la misma, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno de la OPPEA, que puedan poner en entredicho la reputación o imagen de la OPPEA, aunque la información divulgada no sea de naturaleza confidencial.

- Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.

- Se prohíbe codificar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos propiedad de la OPPEA con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos, o con el propósito de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar la información, mensajes o archivo, si no se obtiene previamente el consentimiento por escrito de la Procurador. En el caso de que por razones de seguridad se permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerla, la OPPEA estará facultada para decodificar la misma o restituirla a su condición original, y el usuario será responsable de proveer todos los datos para lograr acceso a la información o archivo.

- Se prohíbe la modificación de los parámetros o configuración de las computadoras de la OPPEA para darle la capacidad de recibir llamadas telefónicas o cualquier otro

tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de la OPPEA.

- Se prohíbe el uso de discos magnéticos o cualquier otro medio de almacenaje de información, sin que haya sido verificado o certificado como libre de virus. Para ello se debe seguir el procedimiento de seguridad previamente establecido.

- Todos los archivos que se creen en las computadoras deben guardarse en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de resguardo (backup) existentes.

- Los usuarios deberán ser automáticamente forzados a cambiar su contraseña periódicamente y un formulario aprobado de mantenimiento de cuenta debe ser sometido al Administrador del Sistema de manera que se solicite cualquier cambio al expediente del usuario.

- Todo el personal con acceso a información computarizada que sea transferido de departamento u oficina o terminado su empleo, sus privilegios de acceso deberán ser terminados el mismo día que termine, sea transferido o promovido.

- Acceso a los sistemas de información del Departamento deberá ser requerido sometiendo un formulario debidamente aprobado de mantenimiento de cuenta del usuario. Cada usuario del sistema de información tendrá una combinación de cuenta/contraseña para acceder los sistemas. Las contraseñas de usuario se utilizarán solamente para el uso del individuo al que se les emitió. El usuario es responsable de proteger su cuenta/contraseña y de cada actividad registrada en el sistema bajo su cuenta.

- Todo el personal es responsable de cumplir con los estándares, políticas, procedimientos y controles establecidos para mantener un ambiente seguro. La Oficina de Sistemas de Información o representante de Seguridad es responsable de monitorear la ejecución de estos requisitos de seguridad.

- El personal deberá devolver la propiedad de la Agencia al cesar sus funciones. El personal es responsable por el uso apropiado y el cuidado de la propiedad que reciban y se comprometen a devolverla cuando terminen su trabajo con la Agencia. Este compromiso es formalizado al firmar el formulario de relevo.

- Los usuarios deben proteger su acceso desactivándose cada vez que dejan su