ESTADO LIBRE ASOCIADO DE PUERTO RICO
DEPARTAMENTO SOMBRILLA
DEL TRABAJO Y RECURSOS HUMANOS
OFICINA DE COMPUTOS Y SISTEMAS DE INFORMACION

POLITICA GENERAL SOBRE LA ADMINISTRACIÓN, MANEJO Y SEGURIDAD DE INFORMACION COMPUTADORIZADA, INTERNET Y MENSAJERIA ELECTRONICA

Edificio Prudencio Rivera Martínez Ave. Muñoz Rivera 505 Hato Rey, Puerto Rico 00918

POLÍTICA SOBRE LA ADMINISTRACIÓN Y SEGURIDAD DE INFORMACIÓN COMPUTADORIZADA, INTERNET Y MENSAJERÍA ELECTRÓNICA

I. BASE JURÍDICA

- ◊ **Ley orgánica del Departamento del Trabajo y Recursos Humanos, Número 15 de 14 de abril de 1931, enmendada**

- ◊ **Ley de Administración de Documentos Públicos de Puerto Rico, Número 5 de 8 de diciembre de 1955, enmendada**

- ◊ **Ley para la Administración de los Recursos Humanos en el Servicio Público del Estado Libre Asociado de Puerto Rico, Número 184 de 3 de agosto de 2004, enmendada**

- ◊ **Código de los Estados Unidos (*US Code*, títulos 17 y 18) y los *Non-Disclosure Agreements*, que prohíben la reproducción, distribución o venta de programas *(software)* y de manuales por medios electrónicos o mecánicos, por ser obra intelectual; para cualquier propósito que no sea, en este caso, el uso oficial.**

II. DEFINICIONES

Los términos o conceptos que se enumeran a continuación tendrán las definiciones siguientes:

A. ***Agencia o agencias***: En singular, se refiere al Departamento del Trabajo y Recursos Humanos. En plural, incluye a los Componentes Operacionales, que se definen más adelante.

B. ***Aplicación***: Programa de computadoras, diseñado para realizar una función determinada.

C. ***Autoridad Nominadora***: "Jefe de agencia con facultad legal para hacer nombramientos para puestos en el Gobierno", según lo define el Artículo 3 de la Ley 184 de 3 de agosto de 2004, enmendada. El Secretario del Trabajo, o los Administradores o Directores de los Componentes Operacionales.

D. ***Código de acceso (password)***: Serie de cifras o símbolos, o una combinación de ambos, que permiten el uso de un sistema o servicio (Por ejemplo: el número 9, para obtener conexión telefónica).

E. ***Contraseña (password):*** Serie de cifras o símbolos, o una combinación de ambos, que identifica al usuario de un sistema o servicio (Por ejemplo: 12CD ó AB34, para acceder a un sistema computadorizado).

F. ***Componentes Operacionales***: Administración del Derecho al Trabajo (en lo sucesivo, ADT), Administración para el Adiestramiento de Futuros Empresarios y Trabajadores (AAFET), Consejo de Desarrollo Ocupacional y Recursos Humanos (CDORH), y Administración de Rehabilitación Vocacional (ARV).

G. ***Departamento***: Departamento del Trabajo y Recursos Humanos.

H. ***Equipos periféricos:*** Equipo electrónico de comunicación de señales o datos que ha sido adquirido por el Departamento y asignado a un empleado con el propósito de mejorar su ambiente de trabajo, mecanizar funciones y procesar información oficial. Por ejemplo: computadora personal *(PC)*, terminal, impresora, módem, escáner, facsímil o líneas de comunicación, entre otros.

I. ***Internet:*** Conjunto de computadoras enlazadas o unidas mediante líneas telefónicas, para el intercambio de información.

J. ***Mensajería electrónica o correo electrónico (e-mail):*** Mensajes que se pueden transmitir -enviar o recibir- por medio de computadoras que están conectadas en una red o entre redes.

K. ***Oficina:*** Centro de Cómputos y Sistemas, Oficina de Informática o de Telecomunicaciones, o sus equivalentes en los Componentes Operacionales.

L. ***Programa (Software):*** Directrices o conjunto de instrucciones que se imparten a un sistema de computadoras o de telecomunicaciones para realizar tareas; a diferencia del equipo *(hardware)*.

M. ***Red:*** Enlace entre computadoras, sistemas o equipos (impresoras, tocadiscos compactos, etc.).

N. ***Servidor:*** Computadora en una red local *(Local Area Network, LAN)* o de corta distancia, para manejar otro equipo conectado a ella. Almacena, dirige y distribuye datos; maneja impresión y trasmisión de datos, como el acceso a

correos de voz, facsímiles, etc.

III. OBJETIVOS

A. Propósito:

1. Garantizar el uso, el manejo, la administración y la preservación de información **oficial del Departamento y sus Componentes Operacionales**

2. Asegurar la integridad y exactitud de la información de las agencias, y protegerla contra su modificación, divulgación, manipulación o destrucción no autorizada, o accidental

3. Asegurar la utilización de la Internet y del sistema de mensajería electrónica **para fines oficiales**, de acuerdo con estándares y normas que protejan la integridad de los datos, su seguridad, y su transferencia a través de los sistemas de computadoras y telecomunicaciones; y como instrumentos suplementarios adecuados para la búsqueda de información sobre nuevas tecnologías, leyes, procedimientos y estándares de ejecución, del Gobierno estatal o federal, universidades o compañías privadas

4. Garantizar la protección de la información personal, confidencial, sensitiva o vital de la agencia, sus empleados y sus beneficiarios o clientes

5. Proveer a Administradores, Secretarios Auxiliares, Directores y Supervisores una base uniforme para la toma de decisiones, en caso de que ocurra mal uso o pérdida de información en la agencia

B. Alcance:

Esta Política aplica al Departamento y sus Componentes Operacionales. Esto incluye:

1. Las oficinas de sistemas de información mecanizados que crean, dan acceso, procesan o custodian la información privilegiada, en oficinas centrales, regionales o de servicios.

2. Los sistemas de computadoras -*mainframes*, sistemas cliente/servidor, minicomputadoras, instalaciones para comunicaciones de datos, redes locales *(LAN), network nodes* de microcomputadoras, computadoras personales o individuales (*desktops* o *notebooks* portátiles), entre otros- que contengan información crítica, confidencial o sensitiva, según ésta sea identificada por las agencias.

3. Las unidades -Negociados, Oficinas, Secciones, Divisiones y otras- y su personal de confianza, de carrera o por contrato, y consultores o asesores en tecnología de información, que trabajen con sistemas de información o con datos que las agencias hayan identificado como críticos, confidenciales o sensitivos. Incluye a agentes de seguridad que dan a otros el derecho de acceso al sistema, analistas, programadores de sistemas y administradores de bases de datos, administradores de redes, asesores en tecnología de información y cualquier otro personal que, según las agencias, tenga acceso a aplicaciones, archivos o programas críticos, confidenciales o sensitivos.

Las normas de acceso a medios electrónicos, Internet y mensajería electrónica serán revisadas periódicamente, en caso de que surjan nuevas necesidades, únicas y particulares del Departamento o sus Componentes Operacionales, o que se implanten nuevas tecnologías. Se considerarán parte de estas normas todos los documentos, los memorandos, las instrucciones, los manuales o las políticas que se notifiquen en el futuro y que sean pertinentes al uso de computadoras u otros equipos relacionados.

Esta Política será de igual aplicabilidad en la utilización de otros recursos de la Internet o Intranet, tales como *www*, FTP, *Chat*, etc.

IV. UTILIZACIÓN DE RECURSOS Y SERVICIOS

A. Servicios disponibles

El Departamento y sus Componentes Operacionales promoverán el buen uso y manejo de los equipos de telecomunicaciones (equipos telefónicos y de datos), la Internet y el correo electrónico; y mantendrán en funcionamiento óptimo la red de telecomunicaciones de nuestro sistema de información, para lo cual se utilizará exclusivamente el personal reclutado con ese fin.

El acceso a la Internet y el correo electrónico se provee a los empleados asignados a labores específicas de servicios, investigación, educación o adiestramiento, mediante conexiones locales o externas, o con países extranjeros. Las locales o externas pueden establecerse con agencias o corporaciones públicas del Gobierno de Puerto Rico o del Gobierno de los EE.UU., o con universidades, colegios y otras instituciones privadas de ambos países. Las que se establezcan con países extranjeros dependerán de que éstos mantengan trato recíproco con el Gobierno de Puerto Rico y de los EE.UU.

Los Directores de unidades de trabajo en las agencias podrán solicitar la adquisición, la instalación, la sustitución o la eliminación de servicios o recursos, de acuerdo con las funciones oficiales y las necesidades de esas unidades. Esto incluye las suscripciones a listas de correo electrónico o páginas

electrónicas, o la participación en grupos noticiosos *(Newsgroups)*, de divulguen información o mensajes, siempre y cuando éstos se utilicen con fines oficiales.

La solicitud se efectuará por escrito al Director de la Oficina de Cómputos y Sistemas; y, si la transacción conlleva gastos, incluirá la autorización de la Oficina de Presupuesto del Departamento o del Componente Operacional que corresponda.

1. Programa de Capacitación

El Departamento y sus Componentes Operacionales mantendrán al día un programa de concienciación, educación y orientación sobre seguridad de información. El propósito de este programa será orientar a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la agencia; y, al mismo tiempo, dar a conocer las reglamentaciones y políticas públicas existentes, y aquellos procedimientos que les conciernen directamente.

Se ofrecerán conferencias a todo nuevo empleado dentro de un lapso no mayor de 30 días desde su comienzo en el trabajo; y a todos los usuarios en todos los niveles, por lo menos anualmente o según las necesidades de las agencias. El período durante el cual se ofrecerán estas conferencias será establecido por el Director de la Oficina, en coordinación con la División de Adiestramiento de la Secretaría Auxiliar de Recursos Humanos o su equivalente en cada Componente Operacional.

B. Manejo de propiedad

La información contenida en las computadoras de la agencia; los servicios asociados, tanto internos como externos; los mensajes de correspondencia electrónica; la información de la Intranet o la Internet; y los documentos y programas existentes, serán adquiridos, instalados, reproducidos, transmitidos, utilizados, almacenados o eliminados, sólo con fines oficiales; y por el personal autorizado para ejercer estas funciones.

Las computadoras, las aplicaciones y los programas, los equipos periféricos y los materiales complementarios o accesorios -como disquetes, filtros, *pen-drives* y otros-, son propiedad de las agencias y no se utilizarán para otros fines que no sean los oficiales.

1. Programación

Toda programación que se desarrolle internamente es propiedad de las agencias, y no puede ser divulgada, copiada o utilizada sin autorización de la Autoridad Nominadora. Se utilizarán productos externos solamente si: 1) han sido adquiridos e instalados legítimamente; 2) las licencias para su uso están

vigentes y; 3) la utilización de estos productos es para mejorar la ejecución de las funciones de las agencias y los deberes de los usuarios; y corresponde a los acuerdos establecidos en el contrato que las agencias negociaron al momento de la compra.

Está prohibido instalar o utilizar programas para los cuales no exista una licencia o autorización de uso válida, a nombre del Departamento o sus Componentes Operacionales; con licencias prestadas de otras computadoras de la agencia; con licencias para uso personal en la residencia de los empleados o por tiempo definido, o adquiridos por otros medios ajenos a los establecidos por las agencias. El uso de una licencia para múltiples computadoras está prohibido, salvo que lo autorice el contrato de las agencias con el fabricante o proveedor.

Todo programa adquirido por el Departamento o sus Componentes Operacionales para utilización en sus sistemas de información electrónicos debe ser registrado correcta e inmediatamente cuando sea recibido, según las indicaciones en su contenido. La Oficina deberá mantener un registro de todos los programas y componentes adquiridos; y guardar y proteger debidamente las licencias y cualquier otra documentación.

Los programas de redes de telecomunicaciones; y los requisitos legales de protección, acceso, almacenamiento y seguridad de estos programas deberán ser controlados por la Oficina de Cómputos y Sistemas. El número total de licencias adquiridas deberá coincidir con el registro (inventario) en el servidor principal.

La Oficina desarrollará un procedimiento centralizado para el resguardo, el control y la administración de programas, licencias y manuales adquiridos. Esta centralización tiene el propósito de minimizar o evitar la pérdida de programas y mantener un control de inventario de los recursos disponibles en el Departamento y sus Componentes Operacionales.

La Oficina deberá mantener documentación (en forma de *log* o bitácora) de cambios, problemas, servicios, mantenimiento, pruebas, modificaciones en programación, violaciones y atentados contra la seguridad de los sistemas.

2. Protección de equipos

a. Acceso a predios

El Departamento y sus Componentes Operacionales establecerán control de acceso del personal a los lugares donde se encuentran las máquinas principales. Toda persona que solicite visitarlos deberá identificarse, y cumplir y respetar todos los procedimientos y las normas establecidas por el

Director de la Oficina, en coordinación con el Oficial de Seguridad.

Se restringirá el acceso a toda persona ajena a las operaciones y el mantenimiento del sistema. La Oficina deberá proveer control de acceso físico adicional, el cual deberá ser conocido y utilizado únicamente por los empleados que trabajan en el área.

b. Instalación de programas o equipos

Las agencias exigirán que todo módulo que vaya a ser instalado al ambiente de producción cumpla con los estándares de calidad existentes.

Todo movimiento de nuevos módulos al ambiente de producción deberá cumplir con los requisitos de control de calidad, documentación, y mantenimiento de un ambiente de procesamiento íntegro y consecuente. Ningún Programador, Operador o consultor podrá realizar por su cuenta movimientos al ambiente de producción sin tomar en consideración los requisitos del proceso, y sin que medie una solicitud escrita del Director de la unidad de trabajo donde se realiza la instalación.

La instalación de programas deberá coincidir con las instrucciones de su manual. Las instalaciones deberán ser hechas por el personal autorizado de la Oficina, y siguiendo las directrices de protección y seguridad descritas. El personal de la Oficina está autorizado a eliminar aquellos programas que no corresponden a los fines de la agencia, que no están incluidos en su inventario o que no estén avalados por un contrato de utilización adquirido por la propia agencia. Esto incluye programas de entretenimiento (juegos) y accesorios para impresoras, computadoras u otro equipo periférico.

No obstante, los sistemas operativos y productos incluidos en la compra de computadoras personales o portátiles, ofrecen la capacidad de ser copiados directamente a disquetes, cartuchos magnéticos o discos compactos (CD). El personal autorizado a realizar esas copias conservará los productos copiados en la Oficina, con el único fin de preservarlos, hasta que sean reinstalados posteriormente. Luego de la reinstalación, borrarán o eliminarán el medio que permite hacer las copias, antes de entregar al usuario la computadora actualizada o reparada.

c. Mantenimiento de equipos de redes o periféricos

El personal de las agencias utilizará equipos electrónicos para facilitar y agilizar el flujo de tareas. Las agencias exigirán que su personal utilice estos equipos correctamente; y que tome las medidas necesarias para protegerlos y mantenerlos funcionando en óptimas condiciones, y evitar daños o averías.

Para que la red de telecomunicaciones funcione aceptablemente, es necesario mantener controles adecuados sobre los inventarios, la ubicación, el mantenimiento y el uso de estos equipos.

Los equipos periféricos deben ser cuidados y utilizados correctamente, para evitar averías causadas por accidentes. Los usuarios no deberán llevar alimentos, ni bebidas, detergentes u otros líquidos, a áreas de trabajo donde existan esos equipos.

Al finalizar el día, los usuarios deberán retirar sus contraseñas de los terminales y computadoras, y apagar todos los equipos electrónicos en su área de trabajo. Toda computadora personal que el usuario deje conectada a la red de telecomunicaciones después de su horario de trabajo, deberá ser desconectada por el supervisor del área.

Cualquier falla en el funcionamiento de los equipos deberá ser notificada inmediatamente al personal de la Oficina que esté a cargo de dar servicio a los mismos, para que los examinen, corrijan la falla o, de ser necesario, ordenen la reparación del equipo.

Toda solicitud de servicio para instalación, configuración, reparación, movimiento o sustitución de equipos, deberá dirigirse por escrito al Director de la Oficina, que asignará al personal autorizado a realizar esas tareas. La eliminación del equipo dañado o sustituido se efectuará en coordinación con el Encargado de la Propiedad de la unidad correspondiente y según las disposiciones vigentes.

C. Controles

1. Controles iniciales

La Autoridad Nominadora designará a las personas autorizadas a adquirir, instalar, modificar, sustituir o utilizar los servicios y recursos disponibles en las agencias; y así constará en la Descripción de Puesto (DTRH-16) de cada funcionario o empleado. Cada una de las unidades de trabajo debe distribuir las tareas de acuerdo con las funciones que realiza cada sección. Antes de autorizar el uso de un acceso de información, el Supervisor del usuario debe asegurarse de que no existe apariencia de conflicto de intereses de los usuarios.

El acceso a estos servicios o recursos por personas ajenas a la agencia (consultores, asesores o Técnicos de Mantenimiento y Servicio) deberá ser controlado adecuadamente para asegurar su buen uso y para restaurar la configuración de las computadoras a su estado original. Estas personas deben ser incluidas en las Listas de Acceso de cada servicio y sus contratos incluirán una cláusula con estos fines.

Las agencias permitirán el acceso a las aplicaciones de producción únicamente a los usuarios que generan transacciones como parte del flujo normal de los servicios ofrecidos. Esos accesos deberán ser regulados de acuerdo con el nivel de seguridad que corresponda a cada usuario.

A aquellos usuarios que ejecutan trabajos que utilizan aplicaciones de producción, se les otorgará acceso sólo para leerlas. Estos usuarios podrán crear nuevas aplicaciones como parte de sus tareas, pero con los parámetros y estandares designados para el ambiente de prueba y desarrollo.

2. Control de cambios

Esta función provee la integración adecuada de recursos, en forma planificada, de todo proceso de cambio en sistemas o módulos existentes; y será realizada por un comité compuesto por representantes de la Oficina de la agencia y sus equivalentes en los Componentes Operacionales. Sus reuniones tendrán el propósito de discutir, analizar y ponderar la revisión de documentación, las necesidades particulares y la aprobación de cambios. Los usuarios del sistema o un representante pueden ser invitados especiales del Comité, según sea necesario.

El Comité presentará los resultados de sus análisis y sus recomendaciones mediante un informe escrito al Secretario del Trabajo. Si éste lo aprueba, la Oficina deberá implantar el cambio recomendado durante los próximos 30 días laborables. Si fuera necesario extender este plazo o si las pruebas realizadas demuestran que el cambio no es viable -por oneroso, por incompatibilidad de los equipos o por otra razón-, el Director deberá notificarlo por escrito e inmediatamente al Secretario del Trabajo, quien autorizará la medida que corresponda.

Algunos de los requisitos para promover el control adecuado en la implantación de cambios, y maximizar la protección y la seguridad de los datos e información son:

◊ Solamente los usuarios autorizados pueden realizar transacciones de mantenimiento en el ambiente de producción.

- ◊ Los Programadores podrán tener acceso de mantenimiento en el ambiente de producción únicamente cuando surja un problema en la producción y sólo hasta que se corrija éste.

- ◊ Los consultores de aplicaciones y de sistemas contratados por la agencia no tendrán acceso a recursos que se encuentren en el ambiente de producción.

- ◊ Las pruebas a módulos de aplicaciones o productos deberán realizarse en el ambiente de prueba y desarrollo.

  Los encargados de pruebas y ejecuciones que se lleven a cabo en el ambiente de prueba no tendrán acceso a recursos en el ambiente de producción. Sin embargo, en aquellos casos en que sea completamente necesario, se condicionará el acceso para que los recursos de producción no puedan ser alterados, en ninguna manera, por las ejecuciones de prueba. Las modificaciones a las aplicaciones deben ser analizadas, aprobadas y trasladadas al ambiente de producción.

3. Auditorías

La Oficina, y la Oficina de Auditoria Interna, se reservan el derecho de vigilar, auditar y fiscalizar los servicios computadorizados, para garantizar que se utilicen para propósitos y gestiones oficiales. Se realizarán auditorías internas, periódicas o al azar, como medida de prevención, cotejando el inventario de los programas aceptados para uso en cada una de las computadoras.

Cualquier empleado, funcionario o supervisor que detecte o presencie un acto que pueda constituir una violación de la legislación o la reglamentación vigentes, o de las disposiciones de esta Política; que cause daños a la propiedad física o intelectual de las agencias; o que ponga en riesgo la integridad o la confidencialidad de la información contenida en los sistemas, deberá notificarlo a la Autoridad Nominadora. Ésta referirá la denuncia a investigación por la Unidad de Seguridad de la Oficina, por la Oficina de Auditoría Interna o, de ser necesario, por la Policía de Puerto Rico.

El resultado de cualquier auditoría rutinaria o de una investigación especial, será informado por el Director de la unidad investigadora, por escrito y con sus recomendaciones, a la Autoridad Nominadora. Si se corrobora falta o delito, la Autoridad Nominadora tomará las medidas pertinentes para detener el acto indebido o ilegal, y evitar que se repita.

D. MANEJO DE INFORMACIÓN

1. Confidencialidad

La información contenida en los sistemas de archivo electrónicos del Departamento y sus Componentes Operacionales, será utilizada con el único propósito de realizar las operaciones propias del servicio público y de las agencias. Ningún funcionario o empleado deberá facilitar información a terceras partes, por ningún concepto que no sea realizar sus funciones como empleado del Departamento o sus Componentes Operacionales.

Ningún usuario podrá leer, revisar o interceptar cualquier tipo de comunicación electrónica oficial o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación; ni enviar a otras personas copias de mensajes de correspondencia electrónica recibidos, sin el conocimiento o consentimiento del remitente original. Tampoco podrá divulgar información, sin importar el medio en que se encuentre, sin autorización previa.

El uso de una contraseña 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; o a información, documento o mensaje creado, recibido o enviado a través del sistema de correo electrónico.

Los terminales de computadora, las microcomputadoras individuales o los *network nodes,* no deben dejarse con cuentas abiertas *(logged on)* en los sistemas de la computadora, si no están atendidos.

2. Acceso

La Oficina establecerá los controles de acceso a sus sistemas electrónicos, de acuerdo con las necesidades de las agencias. La solicitud de acceso deberá indicar el nivel necesario para llevar a cabo la tarea. Será autorizada por el supervisor del usuario y enviada al encargado de los sistemas de información.

La Oficina es responsable de crear y mantener un documento oficial que describa la asignación, el uso, el cambio y el control de las contraseñas. El documento debe permanecer guardado y ser utilizado solamente por el personal autorizado. El documento debe indicar, como mínimo, lo siguiente: 1) los medios de seguridad y el uso de las contraseñas para las máquinas; 2) nombres

de las personas con acceso a cada máquina; 3) período de uso de las

contraseñas; 4) lista de contraseñas por máquina; 5) instrucciones para los cambios de una contraseña inmediatamente después de haber sido utilizada por personal de mantenimiento o servicio, cuando se sospecha de que se ha divulgado a personas ajenas o cuando alguna persona en la lista de acceso termina su empleo en la agencia (por traslado o separación de cualquier índole).

El usuario se identificará adecuadamente cuando acceda al sistema. Esto incluye verificar su autorización cada vez que busque acceso a un nuevo recurso del sistema; evitar que acceda a más de una estación de trabajo a la vez; limitar su acceso a estaciones de trabajo con direcciones específicas; y desconectar automáticamente del sistema al que continúe utilizando una contraseña errónea después de una cantidad específica de intentos.

a. Creación y renovación de contraseñas

El encargado de los sistemas de información o su representante proveerá la solicitud de contraseña, asignándola de acuerdo con los estándares establecidos en la agencia. Las contraseñas pueden ser asignadas en varias etapas de seguridad: 1) acceso a la computadora (antes de acceder a la red); 2) acceso a la red; 3) acceso a los productos, aplicaciones o programas; y 4) acceso específico a leer, escribir, borrar, ejecutar o editar archivos. Estas medidas se implantarán de acuerdo con las necesidades del Departamento y sus Componentes Operacionales.

Las contraseñas deben mantenerse en estricta confidencialidad. Todo usuario que reciba una contraseña será responsable de cumplir con los controles y las políticas de las agencias sobre seguridad de información.

Las agencias proveerán los medios para que se renueve periódicamente la contraseña que cada usuario utiliza para lograr acceso al sistema electrónico. El período de renovación podrá variar, de acuerdo con las necesidades de las agencias, los cambios tecnológicos y los procedimientos establecidos por el encargado de los sistemas de información o su representante.

3. Conservación o disposición

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 *(back-up)* existentes.

Todo documento que haya cumplido con su propósito en las agencias deberá

ser enviado al Archivo Inactivo, de acuerdo con la legislación, la reglamentación y los procedimientos de manejo de documentos o de reciclaje vigentes. Ningún documento podrá ser destruido sin la autorización del Administrador de Documentos de la agencia correspondiente y la Administración de Servicios Generales, el Archivo General de Puerto Rico o cualquier otra entidad con injerencia en ese proceso.

Se dispondrá de los programas, los equipos y los medios de almacenaje (disquetes, discos, etc.) obsoletos de acuerdo con el procedimiento establecido para cualquier otra propiedad de las agencias.

V. PROHIBICIONES Y LIMITACIONES

Además de lo establecido por la legislación y la reglamentación vigentes, y por otras secciones o partes de esta Política, se prohíbe:

A. Utilizar los servicios y recursos descritos con propósitos personales, de recreo, manejo de un negocio o asunto privado del usuario, envío de mensajes en cadena u otros que no estén autorizados; o tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones oficiales.

B. Crear, manejar, enviar o transmitir mensajes o documentos de contenido discriminatorio, ofensivo, obsceno o pornográfico; u opiniones personales sobre raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, o impedimentos físicos o mentales.

   Esta prohibición incluye la instalación de protectores *(screensavers)* con fotos de personas o cualquier otra imagen de significado o contenido sexual, político, racial u otro que pueda considerarse discriminatorio, ofensivo, obsceno o pornográfico; acceso a materiales eróticos; y bromas o cualquier comentario que pueda violar políticas antidiscrimen o sobre hostigamiento.

C. Crear archivos que excedan la capacidad de la cuota del usuario en el servidor o enviarlos mediante el correo electrónico.

D. Realizar actos maliciosos, incluyendo la réplica de virus u otros que puedan afectar adversamente el funcionamiento de los sistemas o los equipos del Departamento, de sus Componentes Operacionales o de otras agencias del Gobierno del Estado Libre Asociado de Puerto Rico.

E. Codificar, asignar contraseñas o modificar de alguna manera información, mensajes de correo electrónico o archivos que sean propiedad del Departamento o sus Componentes Operacionales, con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos; o de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar datos, mensajes o archivos.

   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 Oficina estará facultada para descodificar 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 el archivo.

F. Modificar los parámetros o la configuración de las computadoras para darles la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de las agencias; y modificar los privilegios (derechos de acceso a programas, archivos o directorios) para obtener acceso no autorizado a redes internas o externas.

G. Utilizar discos magnéticos o cualquier otro medio de almacenaje de información que no haya sido verificado o certificado como libre de virus.

H. Retener disquetes u otro medio de almacenaje, o licencias de instalación u otros documentos, sin el debido proceso de registro o sin autorización.

VI. PENALIDADES

Cualquier acto que implique o conlleve la violación de la legislación o la reglamentación vigentes, o de esta Política; o que cause daños a la propiedad física o intelectual de la agencia, o que ponga en riesgo la integridad o la confidencialidad de la información contenida en los sistemas, será investigado por la Unidad de Seguridad de la Oficina y, de ser necesario, por la Oficina de Auditoría Interna del Departamento. El resultado de la investigación será referido, mediante informe con las recomendaciones pertinentes, al Secretario del Trabajo.

Cualquier usuario que incurra en un acto de la naturaleza descrita en el párrafo anterior, se expone a ser sometido a medidas disciplinarias progresivas. Según la gravedad de los actos cometidos, se podrán aplicar sanciones como amonestación escrita, suspensión de empleo o separación; o referir el caso a la Policía de Puerto Rico, el Departamento de Justicia, la Oficina de Ética Gubernamental o cualquier otra institución competente.

VII. SEPARABILIDAD

Si cualquier artículo o inciso de esta Política fuere declarado nulo por un tribunal con competencia, dicha declaración de nulidad no afectará las demás disposiciones, que continuarán vigentes.

VIII. VIGENCIA

Esta Política entrará en vigor inmediatamente después de su aprobación.

En San Juan, Puerto Rico, a 4 de Marzo de 2008.

Román M. Velasco González
Secretario del Trabajo

DEPARTAMENTO DEL
TRABAJO
Y RECURSOS HUMANOS
GOBIERNO DE PUERTO RICO

CERTIFICACION

Certifico que recibí el documento: **Política General sobre la Administración, Manejo y Seguridad de Información Computadorizada, Internet y Mensajería Electrónica.**

Consciente de esta política, me comprometo a dar fiel cumplimiento a la misma y reconozco que estaré sujeto(a) a medidas disciplinarias de no cumplir con las normas establecidas en dicho documento.

_____	_____
Fecha	Firma
_____	_____
Oficina	Nombre (en letra de molde)