

**ESTADO LIBRE ASOCIADO DE PUERTO RICO
INSTITUTO DE CULTURA PUERTORRIQUEÑA**

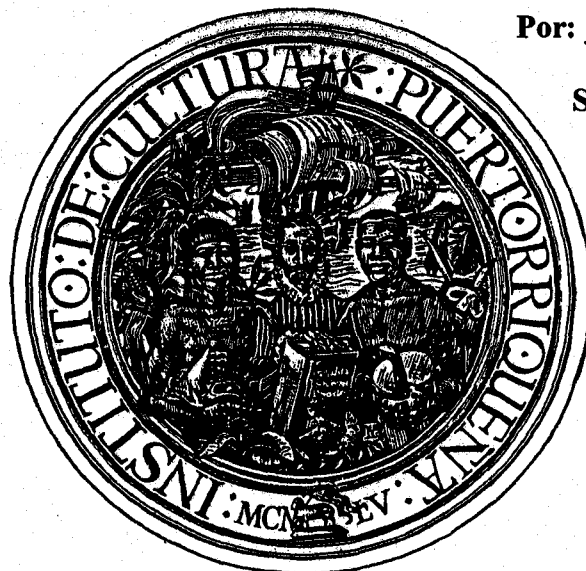
DEPARTAMENTO DE ESTADO

Núm. Reglamento: 6520

Fecha Radicación: 12 de septiembre de 2002

**Aprobado: Ferdinand Mercado
Secretario de Estado**

**Por: Giselle Romero García
Secretaria Auxiliar de Servicios**



**REGLAMENTO PARA LA ADMINISTRACIÓN DE LOS
SISTEMAS DE INFORMACIÓN**

INDICE

CONTENIDO	PÁGINA
ARTÍCULO 1 - INTRODUCCIÓN	1
ARTÍCULO 2 - BASE LEGAL	1
ARTÍCULO 3 - OBJETIVO Y APLICABILIDAD	1
Sección 3.1 - Objetivo	1
Sección 3.2 - Aplicabilidad	1
ARTÍCULO 4 - DISPOSICIONES GENERALES	1
ARTÍCULO 5 - NORMAS SOBRE LA ADMINISTRACIÓN Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	4
ARTÍCULO 6 - GLOSARIO DE TÉRMINOS	13
ARTÍCULO 7 - PROCEDIMIENTOS INTERNOS, DOCUMENTOS Y FORMULARIOS	15
Sección 7.1 - Procedimientos Internos, Documentos y Formularios	15
Sección 7.2 - Documentos y Formularios	15
ARTÍCULO 8 - DEROGACIÓN	16
ARTÍCULO 9 - VIGENCIA	16

ARTÍCULO 1- INTRODUCCIÓN

El Instituto de Cultura Puertorriqueña como parte integral del Gobierno de Puerto Rico preparó e implantó un plan de mecanización en virtud de la Carta Circular Núm. 96-01 emitida por la Oficina de Gerencia y Presupuesto. De esta manera, contribuye al objetivo del Gobierno de lograr la interconexión de los organismos gubernamentales para facilitar y agilizar los servicios al pueblo. Por otra parte, esta iniciativa provee al Instituto de una infraestructura de informática garantizando la agilización de los procesos, así como, la integridad y accesibilidad de la información entre sus componentes.

ARTÍCULO 2- BASE LEGAL

- 1- Ley Núm. 89 del 21 de junio de 1955, según enmendada, Ley que crea el Instituto de Cultura Puertorriqueña.
- 2- Carta Circular Núm. 96-01, según enmendada, emitida por la Oficina de Gerencia y Presupuesto el 13 de noviembre de 1996.
- 3- Carta Circular OC-98-11, emitida por la Oficina del Contralor de Puerto Rico, el 18 de mayo de 1998.

ARTÍCULO 3- OBJETIVO Y APLICABILIDAD

Sección 3.1-Objetivo

Establecer las normas, los procedimientos y las guías generales de control y seguridad para el funcionamiento y operación de la red de sistemas de información del Instituto de Cultura Puertorriqueña con fines de lograr la mejor utilización y efectividad de los mismos.

Sección 3.2- Aplicabilidad

Las disposiciones de este Reglamento aplican a todas las dependencias, programas, oficinas y unidades de trabajo del Instituto, y a todos sus empleados no importa su status o categoría. Aplica, además, a cualquier persona que utilice los sistemas aunque sea de forma esporádica.

ARTÍCULO 4- DISPOSICIONES GENERALES

1. Todos los Sistemas de Información, sus programas, aplicaciones, archivos y equipos electrónicos, el sistema de correspondencia (e-mail), el acceso a la Internet; así como, la documentación y la información desarrollada, tramitada o almacenada en los mismos, es propiedad del Instituto de Cultura Puertorriqueña.

2. 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 uno de los equipos del Sistema del Instituto, será propiedad de la institución 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.
3. Los sistemas y todos sus componentes pueden utilizarse solamente para fines estrictamente oficiales.
4. Ninguna persona podrá utilizar el sistema sin contar con la autorización de la Oficina de Sistemas de Información. Esta mantendrá en el sistema los nombres de las personas autorizadas con los programas que pueden utilizar.
5. La información contenida en los sistemas, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica, la Intranet o la Internet y los documentos y programas existentes, no podrá reproducirse o utilizarse para fines ajenos a las funciones y poderes del Instituto de Cultura Puertorriqueña.
6. La responsabilidad por la seguridad del sistema y de sus componentes es tanto del Instituto como de los usuarios del mismo.
7. Bajo ningún concepto se podrá utilizar los sistemas del Instituto 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 del Instituto para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones del Instituto.
8. Ninguna dependencia, programa u oficina podrá iniciar trámite de compra o adquisición de programas, aplicaciones o equipo electrónico a menos que su petición haya sido evaluada por la Oficina de Sistemas de Información y aprobada por el (la) Director(a) Ejecutivo(a). Cuando surja la necesidad se debe seguir el procedimiento que dispone este Reglamento.

9. La Oficina de Sistemas de Información colocará en la pantalla inicial del sistema una advertencia a los usuarios sobre las disposiciones principales para el uso y control del mismo.
10. El Sistema de Seguridad se implantará de tal manera que no permita a los clientes leer o modificar las aplicaciones.
11. El Instituto de Cultura Puertorriqueña se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de información y de correspondencia electrónica y todos los servicios computadorizados para garantizar que los mismos se utilicen para los propósitos y gestiones relacionados con el trabajo. Las auditorias se pueden realizar periódicamente o al azar o cuando exista una situación en particular que se deba investigar. Lo anterior significa que ningún usuario de los sistemas del Instituto tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través de los sistemas electrónicos de la institución.
12. El Instituto de Cultura Puertorriqueña establece las siguientes políticas para las cuales se dispone prohibición absoluta y cero tolerancia:
 - 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 mensajes que puedan ser catalogados como hostigamiento sexual.
 - b) El manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónico del Instituto. 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 y la política de hostigamiento sexual del Instituto.
 - c) Utilizar protectores de monitores (screen savers) con fotos de personas, atletas, modelos, deportistas o fotos de calendario o cualquier otra imagen que pueda resultar poco seria u ofensiva.
 - d) La divulgación, por cualquier medio, de todo 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.

13. Cumplimiento de las Disposiciones Reglamentarias

- a) Todos los usuarios de los sistemas electrónicos del Instituto vendrán obligados a cumplir con todas las disposiciones de este reglamento y las que emita posteriormente la institución sobre este asunto.

14. Aplicación de Medidas Disciplinarias

- a) Se tomarán las medidas disciplinarias, civiles o criminales, que, correspondan contra los usuarios que violen estas las disposiciones de este Reglamento. La medida a aplicar dependerá de la violación incurrida.
- b) El hecho de que una conducta o actuación relacionada con las computadoras, redes, sistemas y recursos electrónicos del Instituto no esté contemplada en estas disposiciones no impide que se pueda tomar alguna sanción contra el usuario si se determina que se trata de una conducta o actuación imprudente o irresponsable que contraviene los intereses de la institución.

15. Cuando surja la necesidad de revisar o aclarar las políticas establecidas en este reglamento o decretar instrucciones o guías adicionales, la documentación o los memorandos que se emitan, con esos fines, formarán parte de esta reglamentación.

ARTÍCULO 5- NORMAS SOBRE LA ADMINISTRACIÓN Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

1. Confidencialidad de la información

- a) El Instituto establece como política institucional que la información contenida en sus sistemas de archivos electrónicos se utilicen con el único propósito de realizar las operaciones propias que le encomienda la Ley de su creación, así como, para llevar a cabo las mismas de la forma mas óptima posible.
- b) Los empleados vienen obligados a guardar y a proteger la información utilizada para llevar a cabo sus funciones y no podrán facilitar la misma a terceros ni divulgar la información sin previa autorización.

- c) Se prohíbe el envío, fuera del Instituto, de documentos electrónicos o mensajes a través del correo electrónico (e-mail) para evitar poner en peligro la confidencialidad de la información del Instituto.
- d) Se prohíbe el envío o recibo de mensajes de correo electrónico o de cualquier tipo, entre el personal del Instituto y otras personas que no pertenezcan al mismo, en los cuales se divulguen, comenten o expresen hechos u opiniones relacionadas a situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno del Instituto, que puedan poner en entredicho la reputación o imagen de la institución, aunque la información divulgada no sea de naturaleza confidencial.

2. Solicitud de Acceso a los Sistemas

- a) La Oficina establecerá los controles de acceso a los sistemas, de acuerdo con las necesidades de los programas y oficinas.
- b) Cuando algún programa u oficina tenga la necesidad de que alguno de sus empleados accese al sistema, someterá solicitud a la Oficina indicando la necesidad y el nivel de acceso que sea necesario para llevar a cabo la tarea.
- c) La Oficina evaluará la solicitud y aprobará la misma de corroborar la necesidad.

3. Creación de Claves de Acceso

- a) La Oficina creará y asignará la clave de acceso tomando en consideración las responsabilidades y deberes de los empleados.
- b) Todo usuario que reciba una clave de acceso será responsable de mantener en estricta confidencialidad la misma y deberá conocer y cumplir las normas y controles de seguridad establecidos en este reglamento.
- c) El uso de una clave 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 desarrollada, tramitada o almacenada en la computadora que tenga asignada o en cualquier otra.

- d) Se prohíbe modificar los privilegios de acceso a los sistemas para obtener accesos a programas o aplicaciones no autorizadas.
4. Renovación Periódica de las Claves Secretas
- a) Los usuarios deberán cambiar su contraseña cada noventa (90) días.
 - b) Veinte (20) días antes de que concluyan los noventa (90) días aludidos anteriormente, la Oficina comenzará a persuadir al usuario para que cambie su contraseña.
 - c) En aquellos casos en que el usuario no responda a los reclamos de la Oficina, en el término reglamentario, el Sistema le cerrará el acceso automáticamente. Para tener acceso nuevamente al sistema, el usuario deberá llamar a la Oficina para que ésta le asigne una contraseña (password) temporera. Tan pronto se asigne la misma, el usuario deberá entrar su nueva contraseña.
5. Acceso a las Aplicaciones de Producción y de Prueba
- a) Será política del Instituto permitir el acceso a las aplicaciones de producción, únicamente a aquellos usuarios que generen transacciones como parte del flujo normal de los servicios ofrecidos. Esos accesos deberán ser regulados de acuerdo con el nivel de seguridad que cada usuario requiera, según lo determine la Oficina.
 - b) Todo usuario que realice funciones de prueba o desarrollo deberá utilizar el ambiente y los recursos designados para tal propósito (ambiente de prueba).
 - c) La política antes descrita establece que los recursos que componen el ambiente de producción serán permitidos únicamente a los usuarios que, por sus funciones como empleados del Instituto así lo requieran. Solamente aquellas transacciones que se generen como parte del flujo normal de los servicios que ofrece el Instituto, podrán alterar la información oficial contenida en el archivo.
 - d) Las tareas de prueba y desarrollo deberán llevarse a cabo en un ambiente separado y no podrán afectar o alterar de ninguna manera la información oficial.

- e) Aquellos usuarios que utilizan aplicaciones de producción, se les otorgará acceso sólo para leerlas. Estos usuarios podrán crear nuevas aplicaciones como parte de sus tareas, pero bajo los parámetros de nombre designados para el ambiente de prueba y desarrollo.

6. Disposición de Información

- a) Como política institucional se dispondrá, adecuadamente, de la información que nunca más vaya a ser utilizada.
- b) Todo documento (informes, expedientes, memorandos, cartas o de cualquier otro tipo) no importa su forma o medio (físico, electrónico o magnético) que haya cumplido sus propósitos en la institución deberá ser guardado, archivado o destruido de acuerdo con los procedimientos de retención de documentos o de reciclaje establecidos por la Oficina de Administración de Documentos del Instituto.
- c) Se podrá disponer de la información que se almacena en los medios magnéticos y cuyo período de utilización haya terminado, usando los procesos automatizados vigentes.

7. Programa de Concientización

- a) La Oficina de Información del Instituto desarrollará, implantará y mantendrá al día un programa de concientización sobre Seguridad de Información. El propósito del mismo será orientar a los usuarios sobre la importancia de utilizar correctamente el Sistema y sobre la observancia de las normas y controles de seguridad.
- b) Las orientaciones se deben de ofrecer periódicamente, a todos los usuarios en todos los niveles, y podrán variar de contenido dependiendo de las necesidades existentes.

8. Acceso al Área de Máquinas del Sistema de Información

- a) El acceso a las instalaciones donde esté ubicado el Centro de Cómputos de los Sistemas estará controlado por medio de una cerradura electrónica. Sólo el personal de la Oficina conocerá la combinación.

- b) El personal de la Oficina, bajo ningún concepto o razón, podrá divulgar la combinación de la cerradura. Se podrá tomar acción disciplinaria en caso de que se incumpla esta disposición.
- c) La Oficina mantendrá un área de recepción donde deben permanecer los empleados o personas que visiten la Oficina.
- d) Cualquier persona no autorizada que entre al área restringida podrá ser amonestada. En caso dado de que causara cualquier tipo de daño o pusiera en peligro al equipo o a la información del sistema será sancionado de inmediato.

9. Resguardo de Información (Backup)

- a) La Oficina de Sistemas de Información tendrá la responsabilidad de implantar un proceso de resguardo de información para duplicar periódicamente la información procesada. Esta acción se debe efectuar al final de las operaciones, si es posible, diariamente.
- b) La información almacenada debe depositarse en la bóveda del Archivo General.
- c) Los procesos de resguardo de información aplican a todos los sistemas electrónicos existentes en el Instituto. De esta manera, la institución se asegura de continuar los servicios y operaciones de surgir una pérdida de información o un desastre.
- d) Toda información que se reproduzca utilizando tecnología asociada con microfilmación, debe ser ubicada en áreas de acceso controlado y que provean el ambiente adecuado para su almacenaje.

10. Plan de Contingencia

- a) La Oficina de Sistemas de Información tendrá la responsabilidad de desarrollar, implantar y mantener actualizado un plan de contingencia para proteger los sistemas, los equipos y los procesos de operación.
- b) El plan debe contemplar los procesos que sean necesarios para recuperar cualquier segmento de la operación del Centro de Cómputos. Debe proveer también la alternativa, en caso que fuera necesario, de relocalizar las operaciones del Centro de Cómputos en el menor tiempo posible y de la forma más confiable.

- c) La Oficina podrá desarrollar y coordinar simulacros parciales y totales con el propósito de que los usuarios de los sistemas se mantengan preparados y en condición de reaccionar de la mejor forma posible en caso de una emergencia.
- d) El plan de contingencia formará parte de este reglamento. El mismo debe ser revisado y actualizado periódicamente.

11. Pólizas de Seguro

- a) El Instituto de Cultura Puertorriqueña se asegurará que todos los equipos de procesamiento electrónico (centro de cómputos, unidad de telecomunicaciones y microprocesadores) estén cubiertos por una póliza de seguros, que garantice el poder reemplazar los mismos en caso de daños por eventos fortuitos o actos delictivos.
- b) La Oficina debe procurar que el equipo adquirido y en uso sea asegurado por el costo original (costo de reemplazo). En esta cubierta no aplica la depreciación del equipo; por consiguiente, en caso de una reclamación, la compañía aseguradora pagará el costo de reemplazo del equipo tal y como estaba antes de la pérdida, menos el deducible. A través de esta cubierta, la compañía cubrirá los programas (software) y las cintas, disquetes con información o en blanco y el costo de recopilar datos perdidos.
- c) La Oficina preparará un inventario del equipo electrónico que incluya la descripción, el costo por unidad y la localización del mismo. Debe especificar si el equipo es arrendado y el nombre del arrendador. Este inventario se le deberá someter al corredor de seguros asignado para tramitar la póliza.

12. Manejo y Distribución de Informes

- a) El Instituto debe proveer un lugar de ambiente apropiado y seguro para el manejo y distribución de la información que se genera en forma de reportes. Esta clase de información debe ser procesada en un área de acceso limitado y solamente por el personal autorizado. Para llevar a cabo esta función, se crea la Unidad de Control dentro de la Oficina de Sistemas de Información.
- b) Los informes serán separados y clasificados de acuerdo con los parámetros vigentes que se hayan establecido para cada unidad de trabajo. Periódicamente, el personal de la Unidad de Control hará entrega de los informes en las respectivas áreas de trabajo.

13. Instalación de Módulos Nuevos o existentes al Ambiente de Producción o desarrollo de nuevos productos o aplicaciones.

- a) La Oficina se asegurará que todo módulo a ser instalado o toda pieza de programación o codificación nueva o existente a ser modificada y llevada al ambiente de producción, cumpla con los estándares existentes y haya sido sometida a las pruebas correspondientes según el Ciclo de Desarrollo de Sistemas.
- b) Cualquier movimiento de estas piezas al ambiente de producción debe cumplir con los requerimientos de prueba de control de calidad y seguridad, con el estándar de nombres, documentación y con todos los requisitos que el Instituto haya establecido para tal propósito.
- c) Parte del proceso de prueba será establecer los controles de acceso necesarios, probar su efectividad y la interacción del nuevo producto con cualquier subsistema de seguridad existente.
- d) Ningún programador podrá realizar, por su cuenta, movimientos al ambiente de producción sin tomar en consideración los requerimientos que le aplican al proceso.

14. Protección y Cuidado de Equipos Periféricos

- a) La Oficina se asegurará que los programas y oficinas que utilizan equipos electrónicos para facilitar y agilizar el flujo de tareas, requieran de su personal el uso adecuado de los equipos y que tomen todos los cuidados necesarios para protegerlos y mantenerlos funcionando en óptimas condiciones. En caso dado de que un equipo sufra algún desperfecto o trabajo con alguna dificultad, el personal está obligado a llamar a la Oficina para requerir servicio. Deberán seguir los procedimientos correspondientes.
- b) Los servicios de instalación o reparación los llevará a cabo el personal diestro designado para tales funciones. Ningún usuario deberá asumir estas tareas a menos que cuente con la debida autorización de la Oficina.
- c) Los usuarios no deben llevar alimentos sólidos o líquidos (ej. café, refresco, agua, galletitas o cualquier otro tipo de comestible) a las áreas de trabajo donde existan equipos electrónicos o periféricos.

- d) Los usuarios, al finalizar el día, cubrirán los equipos con las cubiertas protectoras (plásticos) que se provean para tal propósito.
- e) En situaciones de emergencia (fuego, terremoto, disturbio atmosférico) los usuarios tomarán las medidas correspondientes para proteger los equipos.

15. Uso de Productos Enlatados

- a) El Instituto utilizará productos "enlatados" (software) en las distintas áreas de trabajo solamente si estos han sido adquiridos legalmente, si las licencias para su uso están vigentes y si la utilización de estos es para mejorar los servicios de la institución.
- b) Se prohíbe a los usuarios: 1) utilizar en los sistemas del Instituto productos enlatados que no estén respaldados por un contrato de utilización adquirido por la institución 2) instalar, usar o tratar de incluir en su estación de trabajo ningún programa de usuario comprado por ellos (ej. screen savers, juegos), pantallas de fondo, trabajos personales, demostraciones de productos o cualquier otro material que no sea provisto por la institución. 3) reproducir producto alguno por ningún tipo de medio como CD, disquetes o cinta que haya sido adquirido por el Instituto y que esté protegido por la Ley de "Copyright".
- c) Todo producto enlatado adquirido por la institución se utilizará exclusivamente en tareas relacionadas con las funciones oficiales de cada unidad de trabajo.

16. Uso de la Red de Telecomunicaciones

- a) Será política del Instituto que los equipos de comunicaciones (equipos telefónicos y de datos) sean usados exclusivamente con propósitos oficiales y que se cumpla con las reglamentaciones y aspectos legales relacionados con el uso de la tecnología.
- b) La utilización de los equipos para la transmisión de datos, no debe representar conflicto de intereses o provecho personal para los usuarios de los mismos.

17. Uso del Correo Electrónico

- a) Se prohíbe a los usuarios del sistema de correo electrónico:
 - 1) Utilizar, durante horas laborables o extendidas, cuentas de correo electrónico distintas a las cuentas oficiales provistas por el Instituto.
 - 2) Enviar a otras personas copia de un mensaje de correspondencia electrónica sin el conocimiento o consentimiento del remitente original.
 - 3) Leer, revisar o interceptar cualquier tipo de comunicación electrónica del Instituto o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.
 - 4) Suscribirse a listas de correo electrónico o que participen en grupos de noticias (newsgroups) que divulguen información o mensajes ajenos a las funciones y deberes del Instituto.

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

18. Reproducción de Programas

- a) Se prohíbe terminantemente la reproducción de cualquier programa enlatado o desarrollado internamente, perteneciente al Instituto, para beneficio personal o de terceras personas o con la intención de afectar de alguna manera los intereses de la institución.

19. Operación de los Equipos Computadorizados y Periféricos

- a) Los equipos computadorizados, las aplicaciones y los equipos periféricos (como impresoras, discos compactos, baterías "ups", terminales y otros bajo esta clasificación) son para el uso exclusivo de los empleados del Instituto que tienen asignados los mismos. Bajo ningún concepto serán utilizados por amigos, visitantes o familiares que estén acompañando al empleado en su área de trabajo.

- b) Los usuarios vienen obligados a leer cuidadosamente todas las instrucciones o advertencias que aparecen o salen en la pantalla y a consultar el Manual de Usuarios para aclarar cualquier duda, sobretodo, cuando la aplicación le dé problemas. Se procederá de esta manera antes de solicitar el servicio a la Oficina.
- c) Ningún equipo podrá salir de una Oficina sin previa autorización de la Oficina de Sistemas.
- d) Bajo ningún concepto se puede mover, instalar o relocalizar cables, componentes o cualquier equipo catalogado como parte de la red de sistemas.
- e) No se permite la reproducción o copia de programas, ni el uso de disquetes o CD's que no sean los provistos por la Oficina para evitar contagio de virus.
- f) Todas las computadoras tendrán instalado un programa de anti-virus que correrá cuando la PC se encienda. Los usuarios vienen obligados a utilizar el mismo diariamente de ser necesario.

20. Guías para la Utilización de los Servicios del Internet

- a) La Oficina de Sistemas de Información será responsable de establecer los procedimientos y la política administrativa para el uso del Internet. La misma deberá revisarse periódicamente en caso de que surjan nuevas necesidades.
- b) Las guías o instrucciones que se emitan para regular el uso del Internet, así como, los memorandos o manuales que se preparen formarán parte de este Reglamento.

ARTÍCULO 6- GLOSARIO DE TÉRMINOS

Instituto

Significa el Instituto de Cultura Puertorriqueña según fue creado por la Ley Núm. 89 21 de junio de 1955, según enmendada.

Director (a) Ejecutivo(a)

Es el (la) Director(a) del Instituto de Cultura Puertorriqueña.

Junta de Directores

Significa la Junta de Directores creada por la Ley Núm. 89 de 21 de junio de 1955, según enmendada.

Oficina

Se refiere a la Oficina de Información del Instituto de Cultura Puertorriqueña.

Dependencia

Se refiere a las áreas programáticas, sedes u oficinas regionales, programas, oficinas, divisiones y unidades de trabajo del Instituto.

Ambiente

Área del computador designada para un uso específico. Los ambientes más conocidos son el de producción y el de prueba. El ambiente de producción es el que utilizan los usuarios para sus funciones diarias.

Aplicación

Es el uso específico que se le da a una programación a través de un computador. Algunos ejemplos de aplicaciones son el archivo de suscriptores o las cuentas por cobrar o pagar.

Banco de Datos

Es una organización electrónica de datos e información que implica la integración de la información a través del ambiente en el cual se utiliza.

Clave de Acceso

Código que utiliza el usuario para comunicarse con el computador. La clave es cualquier grupo de caracteres que identifica a un usuario en el sistema computadorizado.

Equipos Periféricos

Se refiere a impresoras, terminales, Pcs, baterías (Ups), etc.

Nivel de Seguridad o de Acceso

Es el tipo de acceso que el usuario podrá tener a los recursos. Los niveles de acceso más utilizados son: LEER, ACTUALIZAR, CREAR, ELIMINAR, etc.

Programas de Concientización (awareness)

Se refiere a las orientaciones que se ofrecen a los usuarios, en todos los niveles, sobre el uso y control de los sistemas de información.

Plan de Contingencia

Se refiere al grupo de acciones o medidas que tomará la Oficina, conjuntamente con los usuarios del sistema en caso de una emergencia.

Resguardo

Es el proceso en que se reproduce la información contenida en los sistemas y se almacena en un lugar alterno. El propósito es recuperar la mayor cantidad de datos en caso de que se pierda la información contenida en los archivos del sistema.

Usuario

Cualquier persona que utiliza un computador y que está autorizado a leer, entrar o modificar información y programación.

ARTÍCULO 7- PROCEDIMIENTOS INTERNOS, DOCUMENTOS Y FORMULARIOS

Sección 7.1-Procedimientos Internos

1. Se faculta a la Oficina de Sistemas de Información a adoptar formalmente, los procedimientos de funcionamiento interno que estime necesarios para cumplir con las obligaciones y responsabilidades que contraen de conformidad con las disposiciones de este reglamento.

Sección 7.2-Documentos y Formularios

1. La Oficina de Sistemas y diseñará todos los formularios que estime convenientes para las diferentes tareas o acciones que lleve a cabo para la administración de los sistemas.

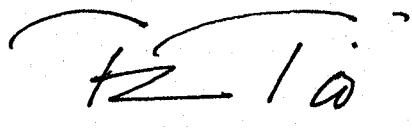
ARTÍCULO 8- DEROGACIÓN

Se deroga cualquier reglamento, norma o procedimiento relacionados con sistemas de información al momento de ser aprobado este reglamento, denominado Reglamento para la Administración de los Sistemas de Información del Instituto de Cultura Puertorriqueña.

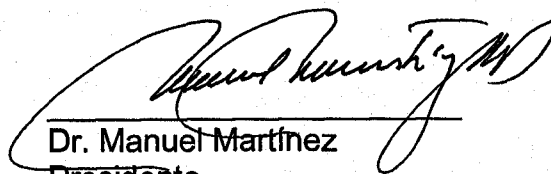
ARTÍCULO 9- VIGENCIA

Este Reglamento entrará en vigor treinta (30) días después de su radicación en el Departamento de Estado, de acuerdo con las disposiciones de la Ley Núm. 170 del 12 de agosto de 1988, según enmendada, conocida como Ley de Procesamiento Administrativo Uniforme del Estado Libre Asociado de Puerto Rico.

Amparados en la facultad que nos confiere la Ley que crea el Instituto de Cultura Puertorriqueña aprobamos este Reglamento hoy, 24 de junio de 2002.



Dra. Teresa Tió
Directora Ejecutiva
Instituto de Cultura Puertorriqueña



Dr. Manuel Martínez
Presidente
Junta de Directores