

REGLAMENTO DE CONTRASEÑAS PARA EL SISTEMA COMPUTADORIZADO DE INFORMACIÓN

Documento Normativo G-0803-010

INTRODUCCIÓN

Nuestro sistema computadorizado de información administrativa se compone de varios subsistemas, a saber: Estudiantes, Recursos Humanos, Finanzas, Recaudaciones, Asistencia Económica y los productos WEB. La actualización de la información en estos subsistemas se realiza a través de estaciones de computadoras personales, ubicadas en las distintas oficinas operacionales con acceso directo al computador central, a excepción de los productos WEB que se pueden acceder desde cualquier lugar del mundo. El acceso al computador central a través de estaciones de trabajo está controlado por la emisión de contraseñas a los empleados de las distintas oficinas para que realicen actividades específicas de acuerdo con la naturaleza de las funciones que desempeñan. La seguridad y la confidencialidad de la información en el sistema computadorizado requieren, por lo tanto, que se adopten estrictas normas para el proceso de emisión y uso de contraseñas.

Artículo I *BASE LEGAL*

Este Reglamento de Contraseñas para el Sistema Computadorizado de Información se promulga en virtud de la autoridad conferida al Presidente por la Junta de Síndicos en sus Estatutos.

Artículo II *ALCANCE*

Este Reglamento aplica a todos los usuarios del Sistema Computadorizado de Información de la Universidad Interamericana de Puerto Rico.

Artículo III *DEFINICIONES*

- 3.1 Ejecutivo Principal – se refiere al Presidente, los Vicepresidentes, los Rectores(as), y los Decanos de Escuelas Profesionales.
- 3.2 Supervisor de Oficina – se refiere a los Directores Ejecutivos y otros funcionarios con funciones de supervisión a nivel de oficina.

Artículo IV *NORMAS GENERALES*

- 4.1 La naturaleza de las funciones que realiza el empleado será la base para determinar si se le autorizan los permisos solicitados. Solamente se les autorizarán permisos solicitados a aquellos empleados cuyas funciones, por su naturaleza, justifiquen tener acceso al sistema mediante los mismos.
- 4.2 La clase de acceso, (búsqueda o actualización) que se autorice en determinada pantalla estará en armonía con las funciones que realiza el empleado y con las de la oficina para la cual trabaja. Esto es, la clase de acceso autorizado no estará en conflicto ni con las funciones del empleado ni con las de la oficina a la cual pertenece. Por ejemplo, a un empleado de la Oficina de Recaudaciones no se le podrá autorizar acceso para hacer cambios en las pantallas que corresponden a las Oficinas de Asistencia Económica ni de Registraduría o viceversa, excepto que en situaciones que lo ameriten y justifiquen, se podrán conceder autorizaciones de acceso temporero.
- 4.3 La contraseña asignada a un empleado es confidencial e intransferible. Permitir su uso por otro empleado o utilizarla en forma indebida será causa para acción disciplinaria.
- 4.4 Tan pronto un empleado cesa en sus funciones, la oficina para la cual el empleado trabaja, ordenará la cancelación de su contraseña.

Artículo V *RESPONSABILIDAD*

- 5.1 Ejecutivo Principal o el funcionario en quien este delegue:
 - 5.1.1 Mediante el formulario "Autorización para acceder Sistema Banner" aprobará la emisión, cancelación o cambio de permisos solicitados para los empleados pertenecientes a su unidad.
 - 5.1.2 Tomará aquellas medidas que sean necesarias para garantizar la mayor seguridad en el uso de estaciones de trabajo y en la confidencialidad de las contraseñas asignadas a los empleados.

5.1.3 Mediante el informe GZRSEC02 que envía trimestralmente el Centro de Informática y Telecomunicaciones, coordinará con la oficina de Recursos Humanos las recomendaciones de los cambios pertinentes, para mantener la seguridad del sistema Banner.

5.2 Supervisor de Oficina:

5.2.1 Mediante el formulario "Autorización para acceder Sistema Banner" recomendará la emisión, cambios o cancelaciones de permisos para los empleados de su oficina para acceder al banco de datos a través de las estaciones de trabajo.

5.2.2 Mantendrá un expediente de los empleados de su oficina que solicitan permisos de acceso.

5.2.3 Actualizará el expediente de empleado con contraseña cuando sea transferido o cese sus funciones en la Institución o justifique cualquier cambio o permisos.

5.2.4 Solicitará para los subsistemas de Finanzas y Recursos Humanos los permisos correspondientes del módulo de seguridad del subsistema para garantizar el uso adecuado de permisos de acceso a la información confidencial.

5.3 Oficina de Recursos Humanos:

5.3.1 Recomendará la cancelación de la contraseña de aquel empleado que la utilice en forma indebida, así como, la acción disciplinaria que corresponda en el caso.

5.3.2 Recomendará la cancelación de su contraseña tan pronto el empleado cesa en sus funciones.

5.3.3 Recomendará los cambios que corresponda en los accesos que permite la contraseña autorizada, tan pronto haya cambio en las tareas que realiza el empleado.

5.3.4 Tomará las medidas necesarias para proteger la confidencialidad de las contraseñas asignadas a los empleados.

5.3.5 Suministrará copia de este Reglamento a cada empleado que se le autorice contraseña de acceso al sistema de información administrativo.

5.3.6 Entregará al usuario copia de la Guía del Usuario de la Red de la Universidad.

5.4 Empleado con contraseña:

5.4.1 Protegerá la confidencialidad de la contraseña que le ha sido asignada. Bajo ninguna circunstancia permitirá que otro empleado la utilice para tener acceso al sistema.

5.4.2 Tan pronto tenga conocimiento de que la contraseña ha perdido su confidencialidad, cambiará su contraseña mediante la pantalla GUAPSWD en el sistema Banner.

5.5 Centro de Informática y Telecomunicaciones:

5.5.1 Asignará contraseña a los empleados a quienes se les haya autorizado oficialmente mediante el formulario "Autorización para acceder Sistema Banner".

5.5.2 Informará al empleado la contraseña que le ha sido asignada mediante el formulario "Asignación Login y Contraseña inicial sistema Banner". El formulario se enviará al empleado en original y sellado. El empleado firmará y desprenderá el talonario enviándolo en sobre sellado al Centro de Informática y Telecomunicaciones, como acuse de recibo de la contraseña. El empleado cambiará su contraseña inicial una vez acceda al sistema, mediante las instrucciones que se encuentran al dorso del documento que retendrá el empleado.

5.5.3 Mantendrá un sistema de seguridad interna que garantice la confidencialidad de las contraseñas asignadas a los empleados de la Universidad.

5.5.4 Informará al Ejecutivo Principal sobre cualquier desviación que se observe en la aplicación de las normas establecidas para autorizar accesos al sistema de información.

5.5.5 Proveerá trimestralmente al Ejecutivo Principal, Director(a) Ejecutivo(a) de Auditoría Interna y Director(a) Ejecutivo(a) de Recursos Humanos Institucional una lista de los empleados con contraseña activa.

Artículo VI ENMIENDAS Y DEROGACIÓN

- 6.1 Este Reglamento deroga la Carta Circular G-74-84 y cualquier otro documento que conflija con las disposiciones del mismo. El Reglamento podrá ser enmendado o derogado por el Presidente de la Universidad.

Artículo VII VIGENCIA

- 7.1 Este Reglamento tendrá vigencia inmediata a partir de su aprobación.

Artículo VIII APROBACIÓN

Presidente

Fecha (D-M-A)

wio