Consejo adm.
Rec. Humanos
Página elect.

Universidad Interamericana de Puerto Rico

22 de diciembre de 2009

Vicepresidentes, Rectores
y Decanos Escuelas Profesionales

Manuel J. Fernós
Presidente

DOCUMENTO NORMATIVO I-1009-002R - REGLAMENTO DE CONTRASEÑAS DE LA UNIVERSIDAD INTERAMERICANA DE PUERTO RICO

Saludos. Le refiero el documento de referencia, el mismo enmienda el Documento Normativo I-1009-002.

Se eliminó la Sección 6.1.3, Pág. 4.

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 necesarios en los accesos autorizados para mantener la seguridad del sistema administrativo de información.

Se corrigió la Sección 6.5.5, Pág. 6, la cual debe leer:

Proveerá **semestralmente al Director Ejecutivo de Recursos Humanos Institucional y a los Directores de Recursos Humanos de los recintos** ~~trimestralmente al ejecutivo principal, al Director Ejecutivo de Auditoria Interna y al Director Ejecutivo de Recursos Humanos Institucional~~ un informe ~~una lista~~ de los empleados con contraseñas activas. La Oficina de Recursos Humanos **indicará** las recomendaciones de los cambios necesarios en los accesos autorizados para mantener la seguridad del sistema administrativo de información.

Cuento con su acostumbrada colaboración en la implantación del mismo.

ymc

Anejo

REGLAMENTO DE CONTRASEÑAS DE LA UNIVERSIDAD INTERAMERICANA DE PUERTO RICO

DOCUMENTO NORMATIVO I-1009-002R

Introducción

Las operaciones de la Universidad Interamericana están altamente mecanizadas y requieren que determinados empleados tengan acceso directo a la base de datos central y, en algunos casos, a bases de datos que se encuentran en entidades o agencias externas a la Universidad. En ambos casos, el acceso está controlado por la concesión de contraseñas a empleados de las distintas oficinas para que realicen actividades específicas de acuerdo con la naturaleza de las funciones que desempeñan. Tanto el acceso de los empleados a los datos que se encuentren en la base central de la Universidad o en su red interna como a los que se encuentren en bases de datos fuera de la Universidad, requieren que se adopten estrictas normas para el proceso de autorización y uso de contraseñas.

I. Base legal

Este Reglamento de Contraseñas se establece en virtud de la autoridad conferida al Presidente de la Universidad por la Junta de Síndicos en los Estatutos de la Universidad y tiene su base en la política establecida en el documento Política Institucional para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones. Además, está en armonía con las leyes internacionales, federales y estatales aplicables.

II. Propósito

Este Reglamento tiene el propósito de establecer las normas para el proceso de autorización y uso de contraseñas para garantizar la seguridad y la confidencialidad de la información. Además, tiene el propósito de asegurar que los usuarios utilicen el acceso concedido a bases de datos, de forma ética, legal y responsable.

III. Alcance

Este Reglamento aplica a todos los usuarios de la Universidad que accedan a cualquier banco de datos interno o externo, como parte de sus funciones.

IV. Definiciones

Para propósitos de este Reglamento, los siguientes términos y expresiones tendrán el significado que se indica a continuación:

4.1 Centro de Informática y Telecomunicaciones (CIT) – la oficina que administra, mantiene y configura las aplicaciones, sistemas de información, redes, telecomunicaciones y las cuentas de los usuarios.

4.2 Contraseña – código de autentificación que utiliza información secreta para controlar el acceso a algún recurso. La contraseña va unida al código de usuario.

4.3 Ejecutivo Principal – los rectores y los decanos de las escuelas profesionales.

4.4 Junta de Síndicos – la Junta de Síndicos de la Universidad Interamericana de Puerto Rico, Inc.

4.5 Oficina Central del Sistema (OCS) – la Oficina del Presidente, los Vicepresidentes y sus directores ejecutivos a cargo de implantar la política institucional, preservar la integridad sistémica universitaria y lograr la coordinación y articulación de sus componentes.

4.6 Presidente – el Presidente de la Universidad Interamericana de Puerto Rico.

4.7 Red interna – la interconexión de las unidades del Sistema Universitario por medio de una infraestructura de telecomunicaciones, redes locales y sus componentes. Puede accederse desde la red externa y la Internet a través de puntos de control como "Firewalls" y "Proxies".

4.8 Supervisor de oficina – los directores ejecutivos y otro personal con funciones de supervisión.

4.9 Unidad – la OCS, los recintos y las escuelas profesionales.

4.10 Universidad o Institución – la Universidad Interamericana de Puerto Rico, Inc.

4.11. Usuario – persona, oficina, organización o grupo de personas a quienes la Universidad permite tener contraseñas para acceder a bases de datos internos o externos.

V. Normas

5.1 La naturaleza de las funciones que realizan los empleados será la base para determinar si se les autorizan las contraseñas solicitadas. Solamente se autorizarán contraseñas a los empleados cuyas funciones, por su naturaleza, justifiquen tener dicho acceso.

5.1.1 La clase de acceso (búsqueda o actualización), que se autorice estará en armonía con las funciones que realizan los empleados y con las de la oficina para la cual trabajan. Por ejemplo, en el caso de acceso a la base central, 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.

5.1.2 En situaciones que lo ameriten y justifiquen, se podrán conceder autorizaciones de acceso temporero.

5.2 Las agencias o entidades externas determinan la clase de acceso que se dará a un empleado de la Universidad para acceder a sus bases de datos.

5.3 Una contraseña autorizada por la Universidad o por una entidad externa a un empleado es confidencial e intransferible. Permitir su uso por otro empleado o utilizarla en forma inapropiada será causa para acción disciplinaria.

5.4 Tan pronto un empleado cese en sus funciones, la oficina para la cual el empleado trabaja tramitará la cancelación de su contraseña. Esto aplicará tanto para contraseñas de la Universidad, como para contraseñas de entidades externas.

VI. Responsabilidades

6.1 Ejecutivo Principal o el funcionario en quien éste delegue:

6.1.1 Mediante el formulario "Autorización para acceder al Sistema Banner" aprobará la concesión, cancelación o cambio de permisos de contraseñas solicitados para los empleados pertenecientes a su unidad.

6.1.2 Tomará las medidas que sean necesarias para garantizar la mayor seguridad en el uso de estaciones de trabajo y en la confidencialidad de las contraseñas de los empleados.

6.2 Súpervisor de oficina:

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

6.2.2 Mantendrá un expediente de los empleados de su oficina que soliciten permisos de acceso.

6.2.3 Mantendrá actualizado el expediente de empleados con contraseñas particularmente cuando sea transferido o cese en sus funciones en la Institución, o se justifique cualquier cambio o permiso.

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

6.2.5 Informará a la oficina de recursos humanos, los casos que detecte de infracciones relacionadas con las normas de contraseñas.

6.2.6 En el caso de contraseñas de la Universidad, solicitará la colaboración del Centro de Informática y Telecomunicaciones de su unidad cuando tenga que acceder a documentos oficiales y el empleado que esté trabajando con ellos se ausente o, por algún otro motivo, no esté disponible.

6.3 Oficina de Recursos Humanos:

6.3.1 Tomará las medidas necesarias para proteger la confidencialidad de las contraseñas de los empleados.

6.3.2 Suministrará copia de este Documento Normativo a cada empleado al que se le autorice contraseña de acceso al sistema de información administrativo o de acceso a una entidad externa.

6.3.3 Entregará al usuario copia del documento Política Institucional para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones.

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

6.3.5 Recomendará la cancelación de la contraseña tan pronto un empleado cese en sus funciones.

6.3.6 Recomendará la cancelación de la contraseña del empleado que la utilice en forma inapropiada, así como la acción disciplinaria que corresponda en el caso.

6.4 Empleado o usuario con contraseña para acceder a bases de datos de la Universidad o de entidades externas:

6.4.1 Acatará la política de la Universidad expresada en el documento Política Institucional para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones, y así como en los documentos normativos relacionados.

6.4.2 Cumplirá con las normas establecidas en este documento.

6.4.3 Protegerá la confidencialidad de las contraseñas autorizadas. Bajo ninguna circunstancia permitirá que otro empleado las utilice.

6.4.4 Tan pronto tenga conocimiento que la contraseña ha perdido su confidencialidad cambiará su contraseña mediante el procedimiento que la Universidad o la entidad externa correspondiente tenga para ello.

6.4.5 Seguirá el siguiente procedimiento para asegurar la confidencialidad de su contraseña:

6.4.5.1 Recibirá del CIT un original sellado con la autorización de su contraseña.

6.4.5.2 El empleado firmará y desprenderá el talonario y lo enviará, en sobre sellado, al Centro de Informática y Telecomunicaciones, como acuse de recibo de la contraseña.

6.4.5.3 El empleado cambiará su contraseña inicial una vez acceda al sistema, siguiendo las instrucciones que se encuentran al dorso del documento, el cual retendrá en sus archivos.

6.5 Centro de Informática y Telecomunicaciones:

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

6.5.2 Informará al empleado la contraseña autorizada mediante el formulario "Asignación *Login* y Contraseña inicial Sistema Banner". El formulario se enviará al empleado en original y sellado.

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

6.5.4 Informará al ejecutivo principal sobre cualquier desviación que se observe en la aplicación de las normas establecidas para autorizar accesos al sistema de información.

6.5.5 Proveerá semestralmente al Director Ejecutivo de Recursos Humanos Institucional y a los Directores de Recursos Humanos de los recintos un informe de los empleados con contraseñas activas. La Oficina de Recursos Humanos indicará las recomendaciones de los cambios necesarios en los accesos autorizados para mantener la seguridad del sistema administrativo de información.

6.5.6 Colaborará con los supervisores de oficina cuando soliciten ayuda para acceder a documentos oficiales y el empleado que esté trabajando con ellos se ausente o, por algún otro motivo, no esté disponible.

VII. Acciones disciplinarias

Cuando se determine que ha habido violación a lo establecido en la Política Institucional para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones o lo dispuesto en otros documentos institucionales, se aplicarán las medidas correctivas y disciplinarias necesarias de acuerdo con la gravedad de la infracción y conforme a las normas establecidas en los documentos oficiales.

VIII. Separabilidad

Si cualquier parte o sección de este reglamente es declarada nula por una autoridad competente, tal decisión no afectará las restantes.

IX. Derogación o enmiendas

Este reglamento enmienda el Documento Normativo I-1009-002 Reglamento de Contraseñas de la Universidad Interamericana de Puerto Rico y cualesquiera otras directrices que estén en conflicto con lo aquí dispuesto. Este documento puede ser enmendado o derogado por el Presidente de la Universidad.

X. Vigencia

Este Reglamento tendrá vigencia inmediata a partir de la aprobación y firma del Presidente.

XI. Aprobación

Manuel J. Fernós, Lcdo.
Presidente

22/12/09
Fecha (D-M-A)

ymc