



10 de diciembre de 2015

CIRCULAR NÚM. 11, AÑO 2015-2016

A LA COMUNIDAD UNIVERSITARIA

Carlos E. Severino Valdez, Ph.D.
Rector

NOTIFICACIÓN DE APROBACIÓN DE POLÍTICA PARA EL CONTROL, USO Y MANEJO DEL SISTEMA ELECTRÓNICO DE CONTROL DE ACCESO

Se informa a la comunidad universitaria la aprobación de la *Política para el Control, Uso y Manejo del Sistema Electrónico de Control de Acceso*, disponible a través del siguiente enlace: <http://opsa.uprrp.edu>.

Esta política incluye el establecimiento de controles para asegurar el uso apropiado y medidas para la implementación adecuada del Sistema de Control de Acceso, las responsabilidades de los funcionarios y los procesos a seguir para la autorización, denegación, duplicados y cancelación de las tarjetas magnéticas multi uso para acceso y de los accesos programados en éstas. La misma va cónsona con la responsabilidad del Recinto de salvaguardar la vida de los miembros de la comunidad universitaria y la protección de la propiedad institucional.

Esta política aplica a todo miembro de la comunidad universitaria que utilice una tarjeta magnética multi uso de acceso a las instalaciones físicas del Recinto, así como a todo el personal responsable del manejo e implementación del Sistema de Control de Acceso en el Recinto.

Para información adicional, pueden comunicarse con la Oficina de Políticas, Sistemas y Auditorías (OPSA), a la extensión 84019.

Cuento con el fiel cumplimiento de la *Política para el Control, Uso y Manejo del Sistema Electrónico de Control de Acceso* para el beneficio de todos.

UNIVERSIDAD DE PUERTO RICO
Recinto de Río Piedras
Rectoría

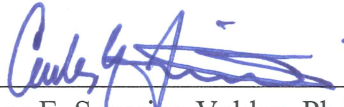
PO Box 23300
San Juan, PR 00931-3300
Tels. 787-763-3930
787-764-0000, Ext. 83000
Fax 787-764-8799



**POLÍTICA PARA EL
CONTROL, USO Y MANEJO
DEL SISTEMA ELECTRÓNICO
DE CONTROL DE ACCESO**

Número: RRP 1 2015-2016

Fecha: 10.12.15

Firma: 

Autoridad Nominadora: Carlos E. Severino Valdez, Ph.D.
Rector

Funcionario Responsable: Decano de Administración

Oficina Responsable: Decanato de Administración

01002715 PM0015 DEL 2015



TABLA DE CONTENIDO

Introducción	3
I. Propósito	4
II. Interpretación y Definiciones.....	4
III. Alcance	6
IV. Responsabilidades.....	6
V. Política	8
A. Declaración De Política	8
B. Disposiciones Generales	8
C. Solicitud de Acceso.....	9
D. Aprobación o Denegación, Cambio y Cancelación de Accesos	10
E. Vigencia	11
VI. Preguntas frecuentes	11
VII. Normativa Legal y/o Institucional aplicable.....	12
VIII. Otras políticas o procedimientos institucionales relacionados	12
IX. Historial.....	12
X. Apéndices, Formularios y Enlaces.....	12
XI. Contactos.....	20



INTRODUCCIÓN

El Decanato de Administración es una unidad que ofrece una diversidad de servicios esenciales a la comunidad universitaria a través de las oficinas y funciones que la componen. Es la unidad encargada y responsable de implementar y velar por el debido cumplimiento de la reglamentación que rige los procesos administrativos del Recinto.

Como unidad institucional autónoma, el Recinto ostenta autonomía académica y administrativa, pero sólo dentro de los entornos establecidos en la Ley de la Universidad, el Reglamento General de la Universidad de Puerto Rico (Reglamento General)¹, las resoluciones de los Cuerpos rectores, la Junta de Gobierno o, en su defecto, las determinaciones que acepte el Presidente de la Universidad de Puerto Rico, en aquello que sea pertinente al Sistema Universitario². La Carta Circular Núm. 92-01 de la Oficina del Presidente de la UPR, informa la Política Institucional sobre Seguridad en la Universidad de Puerto Rico. En ésta, se establecen los procedimientos para promover y mantener un ambiente de estudio y trabajo seguro, libre de riesgos, actos de violencia y peligro. En el ejercicio de su autonomía, el Recinto promulga esta *Política para el Control, Uso y Manejo del Sistema Electrónico de Control de Acceso*. La adopción de esta política va cónsona con la responsabilidad del Recinto de salvaguardar la vida de todos los miembros de la comunidad universitaria y la protección de la propiedad institucional, así como el establecimiento de controles para asegurar el uso apropiado y medidas para la implementación adecuada del Sistema de Control de Acceso.

Haciendo uso de la tecnología como herramienta para alcanzar estos objetivos, el Recinto ha reforzado la seguridad en varias facultades y edificios, mediante la instalación de un Sistema de Control de Acceso operado con tarjetas magnéticas multiuso. Este mecanismo permite: restringir la apertura de puertas o accesos; identificar al usuario de acuerdo con parámetros establecidos; registrar los eventos de acceso por usuario y por puerta; programar la autorización o desautorización del acceso; y funciones adicionales de seguridad y funcionalidad. En esta política se establecen las normas y directrices institucionales para el control, uso y manejo de este sistema y fija las responsabilidades para su implementación.

¹ Reglamento General de la Universidad de Puerto Rico del 2006, Certificación Núm. 90 (2001-02) de la Junta de Síndicos, según enmendada; Reglamento Núm. 6479 del Departamento de Estado del Estado Libre Asociado de Puerto Rico, 25 de junio de 2002.

² Ver Artículo 4(a) de la Ley de la Universidad, 18 L.P.R.A. §603(a)(1) y las Secciones 6.1 y 12.1 del Reglamento General.

**Unidad
Responsable**
Decanato de
Administración

**Unidades
Concernidas**
Decanato de Estudiantes
DSMR
DTAA
OPDF

Acceso en
<http://opsa.uprrp.edu/6ar>

**Fecha de
Efectividad**
10/diciembre/2015





I. PROPÓSITO

Esta política establece las normas institucionales para el manejo, uso e implementación adecuados del Sistema Electrónico de Control de Acceso del Recinto. En ella, se fijan las responsabilidades de los funcionarios y se establecen los procesos a seguir para la autorización, denegación, duplicados y cancelación de las tarjetas magnéticas multi uso para acceso y de los accesos programados en éstas.

II. INTERPRETACIÓN Y DEFINICIONES

Para efectos de esta política, todo término utilizado para referirse a una persona o puesto, se refiere a ambos géneros; el tiempo presente también incluye el futuro. Las palabras y frases empleadas en esta política serán interpretadas según el contexto en que sean utilizadas y según han sido definidas para efectos de la misma. En el caso de aquellas palabras o frases no definidas, éstas tendrán el significado sancionado por el uso común y corriente. Corresponderá, en primera instancia, al Rector, interpretar esta política para resolver cualquier controversia en relación con sus disposiciones o con situaciones no previstas en el mismo.

Acceso	Se refiere al acceso a un área, autorizado mediante solicitud, a un estudiante o personal universitario por el tiempo indicado en la solicitud.
Administrador del Sistema de Control de Acceso	Funcionario designado por el Decano o DOAR a cargo de: custodiar y controlar el inventario de tarjetas, expedir las tarjetas magnéticas multi uso o los duplicados de las mismas a los usuarios autorizados; programar los accesos a las instalaciones en las tarjetas magnéticas multi uso; y eliminar los accesos cancelados en la programación de las tarjetas correspondientes.
Autorización	Acción y efecto de autorizar el acceso solicitado por el estudiante o miembro del personal, según constatado en el formulario de Autorización de Acceso Mediante Tarjeta Magnética Multi Uso .
Cancelación	Dejar sin efecto la autorización de acceso concedida a un Usuario, según constatada en la Notificación De Cambios de Acceso y Cancelaciones , pág. 17.
Decano	Decano de Facultad y/o Escuela
Decano Ejecutivo	Se refiere a decanos que no rigen facultades. Entiendase Decano de Administración, Asuntos Académicos y de Estudiantes.
DOAR	Se refiere a los Directores de las Oficinas Adscritas a Rectoría.



Denegación	Acción y efecto de no conceder autorización del acceso solicitado por un Usuario, según consta en el formulario de Autorización De Acceso Mediante Tarjeta Magnética Multi Uso .
DSMR	Se refiere a la División de Seguridad y Manejo de Riesgos, adscrita a Rectoría, unidad encargada de velar por la seguridad de la comunidad universitaria y la propiedad institucional, así como brindar respuesta inmediata en casos de emergencia en el Recinto.
DTAA	Se refiere a la División de Tecnologías Académicas y Administrativas, unidad adscrita a Rectoría, encargada de mantener los sistemas de información del Recinto.
Recinto	Se refiere a todas las dependencias, predios, terrenos e instalaciones bajo el control del Recinto de Río Piedras de la Universidad de Puerto Rico.
Sistema de Control de Acceso	Es un conjunto de dispositivos mecánicos o electrónicos interactuando entre sí que permite: <ol style="list-style-type: none">1. restringir la apertura de puertas o accesos mediante algún medio mecánico o eléctrico o ambos;2. identificar al usuario de acuerdo con parámetros establecidos para determinar si el acceso es permitido o denegado;3. registrar los eventos de acceso por usuario y por puerta;4. programar la autorización o desautorización del acceso relacionado a cada usuario; y5. permitir funciones adicionales de seguridad y funcionalidad.
Tarjeta Multi Uso	Tarjeta magnética que se utiliza para dar acceso a un usuario a las áreas a las que ha sido autorizado. Incluye las tarjetas de identificación y las tarjetas de acceso a las instalaciones.
Unidad	Se refiere a Decanatos, Oficinas y/o Divisiones del Recinto de Río Piedras.
Usuario	Persona autorizada a tener acceso a una instalación universitaria mediante el uso de una Tarjeta Magnética multi uso. Incluye estudiantes que estén matriculados en el Recinto.



III. ALCANCE

Esta política aplica a todo miembro de la comunidad universitaria que utilice una tarjeta magnética multi uso de acceso a las instalaciones físicas del Recinto. Además, aplica a todo el personal responsable del manejo e implementación del Sistema de Control de Acceso en el Recinto.

IV. RESPONSABILIDADES

**Decano, Decano
Ejecutivo y/o DOAR**

1. Vela por el fiel cumplimiento de esta política en su unidad.
2. Recibe las solicitudes de autorización de acceso y evalúa la acción a tomar para asegurarse que la naturaleza de las funciones u horario del usuario/solicitante, amerita la concesión del acceso durante el horario solicitado.
3. Autoriza, deniega o cancela los accesos solicitados por los Usuarios.
4. Designa al funcionario que fungirá como administrador del sistema de acceso.

**Director DSMR o
Representante**

1. Vela por el fiel cumplimiento de esta política.
2. En coordinación con el Administrador del Sistema de Control de Acceso, evalúa las áreas en las cuales se instalará el Sistema de Control de Acceso y hará recomendaciones al respecto.
3. Supervisa el funcionamiento del Centro de Monitoreo del Sistema.
4. En caso de reportarse hurto de tarjeta, contactará a la Policía de Puerto Rico para radicar querrela.

**Administrador del
Sistema de Control
de Acceso**

1. Verifica que el uso y manejo del sistema se realice adecuadamente.
2. Protege y mantiene en un área bajo llave las tarjetas de acceso y conserva un registro y control de inventario de las tarjetas recibidas (Apéndice 4).
3. Expide las tarjetas magnéticas multi uso para acceso así como los duplicados, según establecido en esta política.
4. Facilita la coordinación de adiestramiento y asistencia al personal y/o estudiantado de su unidad sobre el uso adecuado de la tarjeta.
5. Notifica a los usuarios, cuando sea necesario, de interrupciones en el sistema para el mantenimiento del servidor.
6. Asegura la pronta respuesta a emergencias y acceso adecuado a las instalaciones por el personal de servicio de apoyo.
7. Facilita el acceso temporero a Contratistas o Compañías de Mantenimiento, Personal de Emergencias Estatal u otros.



8. Identifica y marca de forma única, las tarjetas de acceso.
9. Conserva un registro de los accesos solicitados, otorgados, denegados y cancelados.
10. Realiza una revisión de las tarjetas de acceso y los lugares accedidos anualmente.
11. Prepara informes sobre acceso a determinadas áreas a solicitud del Decano o la DSMR.

**Funcionario del
Decanato de
Estudiantes**

1. Utilizará tarjetas de identificación de estudiantes que sean compatibles con las tarjetas de acceso, de manera que las mismas se puedan programar para autorizar al estudiante la entrada a un área específica.
2. Emite y reemplaza las tarjetas magnéticas multi uso a estudiantes.

Supervisor

1. Evalúa la necesidad de acceso del personal nuevo o existente.
2. Notifica al Administrador de Control de Acceso cuando haya un cambio significativo en las funciones del usuario bajo su responsabilidad, que amerite hacer una revisión a los accesos concedidos a un usuario.

**DTAA (DOAR) o
funcionario
designado**

1. Supervisa la infraestructura de las telecomunicaciones en las instalaciones para el funcionamiento adecuado del Sistema de Control de Acceso.
2. Determina la compatibilidad entre equipos para que su adquisición sea costo efectiva.
3. Brinda apoyo al momento de la instalación de la aplicación en los servidores.
4. Supervisa las Compañías que brindarán mantenimiento al Sistema desde el componente de informática.

**Usuario y/o Custodio
de Tarjeta**

1. Responsable de mantener el uso adecuado de los accesos concedidos a las instalaciones; evitando además facilitar el acceso a personas no autorizadas.
2. No prestará a persona alguna su tarjeta de acceso.
3. Notifica al Administrador del Sistema, toda vez que culmine el periodo para el cual esté autorizado a utilizarla o ya no requiera de su uso; para que proceda a la cancelación del acceso.
4. En caso de pérdida de la tarjeta de acceso, notificará inmediatamente al Administrador de Control de Acceso; en el caso de empleados informará también a su supervisor. Además, radicará una querrela en la DSMR para informar la pérdida; según expresa la sección **V (D) de ésta política-Aprobación o Denegación, Cambio y Cancelación de Accesos.**



5. Una vez obtenga de la facultad la certificación sobre pérdida de la tarjeta, efectuará el pago correspondiente en la Oficina de Recaudaciones antes de solicitar el reemplazo. Debe presentar evidencia de pago al solicitar el reemplazo.

V. POLÍTICA

A. Declaración De Política

Es política institucional de la Universidad de Puerto Rico promover y mantener un ambiente seguro de trabajo, estudio e investigación. En atención al interés institucional en la seguridad de la comunidad universitaria y la protección de la propiedad, el Recinto procura implantar medidas para evitar los accesos no autorizados a sus instalaciones. Además, se propone establecer controles internos para salvaguardar la integridad del proceso de distribución de tarjetas magnéticas multi uso para acceso y controlar los accesos a los espacios universitarios programados en éstas, todo ello sin menoscabar las necesidades de uso de la comunidad universitaria.

Para cumplir con lo anterior, el Recinto adopta y promulga esta Política para el Control, Uso, Manejo del Sistema Electrónico de Control de Acceso.

B. Disposiciones Generales

1. El Sistema de Control de Acceso (en adelante, el “Sistema”), es un conjunto de dispositivos mecánicos o electrónicos interactuando entre sí, que permite:
 - a. restringir la apertura de puertas o accesos mediante algún medio mecánico, eléctrico o ambos;
 - b. identificar al usuario de acuerdo con parámetros establecidos para determinar si el acceso es permitido o denegado;
 - c. registrar los eventos de acceso por usuario y por puerta;
 - d. programar la autorización o desautorización del acceso relacionando a cada usuario; y
 - e. permitir funciones adicionales de seguridad y funcionalidad.
2. Una vez entregada la tarjeta de acceso al Usuario, éste asume la custodia y, por tanto, la responsabilidad exclusiva sobre su uso y protección adecuados. El uso inadecuado o los daños ocasionados por el mal uso del acceso concedido conllevará las sanciones que estipula la reglamentación vigente en el Recinto de Río Piedras.
3. Se activará sólo una tarjeta magnética multi uso de acceso por persona durante el periodo que determine la unidad que programa o concede el acceso. La misma será desactivada al culminar el periodo por el cual fue otorgado dicho acceso. En el caso de empleados este termino será la separación del servicio.



4. En el caso de los estudiantes, el Decanato de Estudiantes estará a cargo de la gestión de producción y entrega de las tarjetas. En el caso de empleados, esta responsabilidad recaerá en la Oficina de Recursos Humanos.
5. El costo de reemplazo de la tarjeta será asumido por el usuario si se demuestra que fue mutilada por negligencia en el uso de la misma. En caso de deterioro no se impondrá cargo alguno. Si la solicitud de reemplazo responde a situaciones de apropiación ilegal o perdida se procederá según la sección **D** incisos **9** y **10** de esta política.
6. Cada unidad institucional será responsable de establecer los procedimientos y controles internos apropiados, conforme sus necesidades particulares para el manejo adecuado del sistema. Los mismos no pueden ir en contra de alguna disposición de esta política.

C. Solicitud de Acceso

1. El solicitante completará en todas sus partes el formulario **Autorización De Acceso Mediante Tarjeta Magnética Multi Uso**, (**Apéndice 1**), si es estudiante; en el caso de empleados (**Apéndice 2**), y lo entregará al Administrador del Sistema de su Unidad, en adelante “el Administrador”.
2. Al firmar el documento formulario **Autorización de Acceso Mediante Tarjeta Magnética Multi Uso**, el usuario reconoce y acepta que:
 - a. el acceso solicitado será para el uso específicamente indicado en el documento y durante el periodo otorgado;
 - b. la tarjeta de acceso no es de carácter transferible, es decir: la misma es para uso exclusivo del usuario a quien se le concede acceso; y
 - c. se compromete a notificar cualquier cambio que surja en los datos suplidos en el formulario de autorización.
3. El Administrador examinará el formulario para constatar que:
 - a. el mismo fue firmado y completado en todas sus partes;
 - b. indique la clasificación del usuario: en el caso de estudiantes, si es graduado o subgraduado, y si es empleado Docente o No docente;
 - c. los accesos solicitados estén justificados a base de la necesidad; y
 - d. la legitimidad de la autorización de los accesos solicitados - para ello requerirá al usuario mostrar una identificación con foto.
4. En el caso de estudiantes, el formulario de autorización de acceso a laboratorios de investigación o salones debe ser aprobado y firmado por los profesores responsables de la supervisión del estudiante en la instalación.



5. El Administrador referirá el formulario **Autorización de Acceso Mediante Tarjeta Magnética Multi Uso** al Decano, Decano Ejecutivo y/o DOAR para la autorización correspondiente.

D. Aprobación o Denegación, Cambio y Cancelación de Accesos

1. Luego de evaluar el formulario, el Decano, Decano Ejecutivo y/o DOAR autorizará o denegará los accesos solicitados.
2. Si por alguna razón el Decano, Decano Ejecutivo y/o DOAR entiende que la persona solicitante no tiene una razón legítima para obtener acceso al espacio físico u horario solicitado, podrá proceder a denegar el mismo. Una razón legítima para no otorgar acceso a un espacio físico es cuando, por ejemplo, el solicitante no tiene clase o laboratorio en el lugar al cual solicita acceso.
3. Una vez aprobado el acceso el Administrador estará a cargo de la programación y activación de las tarjetas. Llevará un registro de las tarjetas entregadas y los accesos concedidos, **Inventario de Tarjetas Magnéticas Multi Uso Entregadas (Apéndice 4)**.
4. Cuando el acceso concedido a un usuario pueda levantar preocupación o posible conflicto, se suspenderá el mismo hasta tanto el Decano de Facultad, Decano Ejecutivo y/o DOAR o funcionario designado en conjunto con la DSMR realice una evaluación y/o investigación y para determinar la continuidad o cancelación permanente de este.
5. Cualquier cambio de horario en la programación del acceso asignado debe ser solicitado y justificado por el Usuario y ser autorizado por el Decano, Decano Ejecutivo y/o DOAR. El Usuario deberá completar el formulario **Notificación de Cambio de Acceso y Cancelaciones** (Apéndice 3).
6. Es responsabilidad exclusivamente del Administrador, verificar y asegurarse de que los accesos concedidos a estudiantes se cancelen al concluir el término de vigencia que le fue otorgado.
7. En el caso de renuncia de empleados o separación del servicio, el supervisor del empleado se asegurará de que éste complete el formulario de **Notificación de Cambio de Acceso y Cancelaciones** (Apéndice 3) y se remita al Administrador de su unidad.
8. Cada Administrador establecerá, conforme las necesidades de su área, el término de tiempo requerido para la cancelación de cualquier acceso concedido y no utilizado.
9. En caso de robo, apropiación ilegal o pérdida de la tarjeta de acceso, el Usuario deberá notificar inmediatamente al Administrador de su unidad. Si la situación



ocurre en los predios del Recinto, durante horas no laborables notificará a la DSMR para que procedan con la cancelación del acceso y preparen la querrela correspondiente. De ocurrir fuera del Recinto, radicará primero una querrela en Policía y presentará copia de la misma al momento de radicar la querrela en la DSMR para luego solicitar un reemplazo.

10. Llenará un nuevo formulario de **Autorización de Acceso Mediante Tarjeta Magnética Multi Uso** para obtener un duplicado, efectuará el pago correspondiente en la Oficina de Recaudaciones y presentará el recibo de pago al Administrador.

E. Vigencia

Esta política entrará en vigor una vez sea aprobada y firmada por el Rector y divulgada a la comunidad universitaria.

VI. PREGUNTAS FRECUENTES

1. ¿Qué debo hacer para obtener mi tarjeta magnética multi uso?

Estudiante: En caso de los estudiantes, el Decanato de Estudiantes estará a cargo de la gestión de entrega. Si no posee tarjeta multi uso, solicitará la misma en el lugar (Facultad, Residencia, Salón y/o Laboratorio) para el cual necesita acceso.

Empleado: En caso de los empleados, la Oficina de Recursos Humanos estará a cargo de la entrega.

2. ¿Qué debo hacer para que me programen los accesos que necesito en mi tarjeta magnética multi uso?

El solicitante completará en todas sus partes el formulario **Autorización De Acceso Mediante Tarjeta Magnética Multi Uso**, (Apéndice 1) si es estudiante; (Apéndice 2) en el caso de empleados, y entregará al Administrador del Sistema de Control de Acceso de su Unidad.

3. ¿Que debo hacer si pierdo la tarjeta de control de acceso?

En caso de que la tarjeta de acceso sea robada o extraviada, el Usuario deberá notificar inmediatamente al Administrador del Sistema de su área para que sea desactivada. Cuando sea robada en los predios del Recinto, debe presentar una querrela a la DSMR. Si la tarjeta es robada fuera del Recinto, debe radicar una querrela en la Policía, traer copia de la misma y registrar la querrela en la DSMR antes de solicitar reemplazo.



VII. NORMATIVA LEGAL Y/O INSTITUCIONAL APLICABLE

1. Ley Núm. 1 del 20 de enero de 1966, según enmendada, mejor conocida como la *Ley de la Universidad de Puerto Rico* 18 LPRA § 601 *et seq.*
2. *Reglamento General de la Universidad de Puerto Rico del 2006*, Certificación Núm. 90 (2001-2002) de la Junta de Síndicos, según enmendada.
3. *Reglamento General de Estudiantes de la Universidad de Puerto Rico del 29 de agosto de 2009*, Certificación Núm. 13 (2009-2010) de la Junta de Síndicos, según enmendada
4. *Reglamento para el Control de la Propiedad Mueble de la Universidad de Puerto Rico*, Certificación Núm. 62 (1994-1995) de la Junta de Síndicos, según enmendada
5. *Carta Circular 92-01 de la Oficina del Presidente, Política Institucional sobre Seguridad en la Universidad de Puerto Rico del 28 de mayo de 1992*

VIII. OTRAS POLÍTICAS O PROCEDIMIENTOS INSTITUCIONALES RELACIONADOS

1. *Procedimiento para la Solicitud y Control de Llaves de las Instalaciones Físicas del Recinto de Río Piedras (RP-79) rev. Junio 2007*
2. *Política para la Formulación y/o Revisión Sustancial de Políticas y/o Procedimientos en el Recinto*, Iro. de marzo de 2013, Rectora Ana R. Guadalupe Quiñonez, Ph.D.

IX. HISTORIAL

- *Política para el Control, Uso y Manejo del Sistema de Control de Acceso Electrónico en el Recinto de Río Piedras*, [fecha de aprobación], Rector Carlos E. Severino Valdez, Ph.D.

X. APÉNDICES, FORMULARIOS Y ENLACES

APÉNDICES

- **APÉNDICE 1** - Autorización De Acceso Mediante Tarjeta Magnética Multi Uso - Estudiantes
- **APÉNDICE 2** - Autorización De Acceso Mediante Tarjeta Magnética Multi Uso - Empleados
- **APÉNDICE 3** – Notificación de Cambios a los Accesos y Cancelaciones
- **APÉNDICE 4** – Inventario de Tarjetas Magnéticas Multi Uso Entregadas

ENLACES

- Portal de la División de Seguridad y Manejo de Riesgos: <http://seguridad.uprrp.edu/>



Apendice 1 **RECINTO DE RÍO PIEDRAS**
DIVISIÓN DE SEGURIDAD Y MANEJO DE RIESGOS

Original-Oficina de origen
 Copia – solicitante
 Rev. octubre /2015

Autorización De Acceso Mediante Tarjeta Magnética Multi Uso Estudiantes

Nueva Reemplazo

SOLICITUD NÚM. _____

FECHA SOLICITUD _____

(1)Nombre del Solicitante		(2)Número de Estudiante: ____ - ____ - ____	
(3)Dirección Residencial/Hospedaje			
(4)Dirección Postal (si diferente a la residencial)			
(5)Clasificación del Estudiante: <input type="checkbox"/> Sub Graduado <input type="checkbox"/> Graduado		(6)Término de Vigencia ____ Semestre ____ - ____	
(7) Facultad y Departamento		(8)Teléfono de Contacto:	

(9)DESCRIPCIÓN DE ACCESOS SOLICITADOS			Aprobado	
EDIFICIO	TALLER/LABORATORIO/SALÓN	HORARIO	Si ✓	No ✓

CERTIFICACIÓN

Certifico que la información provista está completa y correcta; que he recibido una tarjeta magnética de control de acceso y me comprometo a cumplir con las disposiciones de la *Política de Control, Uso y Manejo del Sistema de Control de Acceso Electrónico en el Recinto de Río Piedras* a la cual podré acceder a través de [<http://opsa.uprrp.edu/6ar>]. Utilizaré la tarjeta magnética para los usos autorizados solamente y durante el periodo otorgado, según consta en este formulario. En caso de pérdida de la tarjeta se notificará al Administrador del Sistema de Control de Acceso de mi Escuela o Facultad, y en caso de robo notificaré además a DSMR y radicaré querrela a la Policía de Puerto Rico.

Administrador del Sistema de Control de Acceso	
_____ Firma del Receptor	_____ Nombre en letra de molde
_____ Fecha	_____ Firma
_____ Fecha	_____ Fecha

(10) PARA USO DEL ADMINISTRADOR DEL SISTEMA		
Solicitud Recibida por:	Tarjeta entregada por:	Número de Serie de Tarjeta _____
_____	_____	Nueva <input type="checkbox"/> Reemplazo <input type="checkbox"/>
Fecha	Fecha	Núm. Recibo pago reemplazo

(11) EN CASO DE LABORATORIOS	
Edificio: _____	Laboratorio: _____
Profesor/Investigador Responsable	_____
_____	Firma
Letra de Molde	_____
	Fecha

INSTRUCCIONES GENERALES

Este formulario debe ser completado en todas sus partes y firmado por toda persona que solicite acceso a áreas o unidades del Recinto controladas por mecanismos electrónicos de acceso operados mediante tarjeta magnética multi uso. El mismo debe ser aprobado por el Director de Departamento/Decano de Facultad, Escuela o su Representante. En el caso de laboratorios debe estar firmado por el Profesor/Investigador a cargo del área.

Instrucciones Específicas:

- (1) Nombre del Solicitante: se explica solo.
- (2) Número de Estudiante: se explica solo
- (3) Dirección Residencial/Hospedaje: lugar donde reside o se hospeda mientras estudia.
- (4) Dirección Postal (si diferente a la residencial): dirección en la que recibe la correspondencia.
- (5) Clasificación del Estudiante: indique si es graduado o sub graduado.
- (6) Término de Vigencia: indique el semestre y el año en curso en que radica solicitud.
- (7) Facultad y Departamento: Facultad y Departamento al cual fue admitido para obtener un grado.
- (8) Teléfono de Contacto y Correo Electrónico: Número de celular u hospedaje y dirección de correo electrónico actualizados
- (9) Descripción de Accesos Solicitados: área de acceso controlado por tarjeta magnética para la cual solicita acceso
- (10) Para Uso del Administrador del Sistema: en esta sección el Administrador del sistema indica la persona que recibe la solicitud, quien entrega la tarjeta, así como las fechas, número de codificación de la tarjeta y el recibo de pago en caso de que la solicitud sea para reemplazo.
- (11) En caso de Laboratorios: ésta sección debe ser completada por el Profesor/Investigador encargado del laboratorio para el cual el estudiante solicita acceso.
- (12) Denegación, Cancelación de Accesos: en esta sección se describen las razones para denegar o cancelar un acceso.



Autorización De Acceso Mediante Tarjeta Magnética Multi Uso
Empleados

SOLICITUD NÚM. _____

FECHA SOLICITUD _____

Nueva Reemplazo

(1)Nombre del Solicitante		(2) Identificación con foto: <input type="checkbox"/> Licencia de Conducir <input type="checkbox"/> Tarjeta Electoral	
(3)Dirección Residencial			
(4)Dirección Postal (si diferente a la residencial)			
(5)Clasificación del Empleado: <input type="checkbox"/> Docente <input type="checkbox"/> No docente <input type="checkbox"/> Visitante			(7)Término de Vigencia
(6)Puesto: _____			_____
(8) Facultad, Escuela y Departamento u Oficina		(9)Teléfono de Oficina, Extensión o Núm. Celular:	

(10)DESCRIPCIÓN DE ACCESOS SOLICITADOS			Aprobado	
EDIFICIO	LUGAR QUE ABRIRÁ/OFICINA	HORARIO	Si ✓	No✓

CERTIFICACIÓN

Certifico que la información provista está completa y correcta; que he recibido una tarjeta magnética de control de acceso y me comprometo a cumplir con las disposiciones de la *Política de Control, Uso y Manejo del Sistema de Control de Acceso Electrónico en el Recinto de Río Piedras* a la cual podré acceder a través de [<http://opsa.uprrp.edu/6ar>]. Utilizaré la tarjeta magnética para los usos autorizados solamente y durante el periodo otorgado, según consta en este formulario. En caso de pérdida de la tarjeta se notificará al Administrador del Sistema de Control de Acceso de mi unidad, y en caso de robo notificaré además a DSMR y radicaré querrela a la Policía de Puerto Rico.

Administrador del Sistema de Control de Acceso	
_____	_____
Firma del Receptor	Nombre en letra de molde
_____	_____
	Firma
_____	_____
Fecha	Fecha

(10) PARA USO DEL ADMINISTRADOR DEL SISTEMA:		
Solicitud Recibida por:	Tarjeta entregada por:	Número de Serie de Tarjeta
_____	_____	_____
_____	_____	Nueva <input type="checkbox"/> Reemplazo <input type="checkbox"/>
Fecha	Fecha	Núm. Recibo pago reemplazo

INSTRUCCIONES GENERALES

Este formulario debe ser completado en todas sus partes y firmado por toda persona que solicite acceso a áreas o unidades del Recinto controladas por mecanismos electrónicos de acceso operados mediante tarjeta magnética multi uso. El mismo debe ser aprobado por el Director de Departamento/Decano de Facultad, Escuela o su Representante.

Instrucciones Específicas:

- (1) Nombre del Solicitante: se explica solo.
- (2) Identificación con foto: marque si el empleado presentó licencia de conducir o tarjeta electoral (para verificación de identidad).
- (3) Dirección Residencial: dirección física o lugar donde reside.
- (4) Dirección Postal: (si diferente a la residencial): dirección en la que recibe la correspondencia.
- (5) Clasificación del Empleado: indique si es Docente, No docente o Visitante.
- (6) Puesto: se explica solo.
- (7) Término de Vigencia: indique el periodo que comprende la aprobación del acceso.
- (8) Facultad y Departamento: Facultad y Departamento donde realiza las tareas como empleado del Recinto.
- (9) Teléfono de Oficina, Extensión o Núm. celular y Correo Electrónico: Número de contacto en la oficina, celular y dirección de correo electrónico actualizados.
- (10) Descripción de Accesos Solicitados: áreas de acceso controlado por tarjeta magnética para la cual solicita acceso.
- (11) Para Uso del Administrador del Sistema: en esta sección el Administrador del sistema indica la persona que recibe la solicitud, quien entrega la tarjeta, así como las fechas, número de codificación de la tarjeta y el recibo de pago en caso de que la solicitud sea para reemplazo.
- (12) Denegación, Cancelación de Accesos: en esta sección se describen las razones para denegar o cancelar un acceso.



Apendice 3

Original-Oficina de origen
Copia – solicitante
Rev. octubre 2015

**UNIVERSIDAD DE PUERTO RICO
RECINTO DE RÍO PIEDRAS
DIVISIÓN DE SEGURIDAD Y MANEJO DE RIESGOS**

Notificación De Cambios de Acceso y Cancelaciones

SOLICITUD NÚM. _____

FECHA SOLICITUD _____

(1)Nombre del Solicitante		(2) Identificación con foto: <input type="checkbox"/> Licencia de Conducir <input type="checkbox"/> Tarjeta Electoral o #de estudiante (si aplica) ____-____-____	
(3)Dirección Residencial			
(4)Dirección Postal (si diferente a la residencial)			
(5)Clasificación del Solicitante: <input type="checkbox"/> Visitante		(6)Término de Vigencia	
EMPLEADO: <input type="checkbox"/> Docente <input type="checkbox"/> No docente	ESTUDIANTE: <input type="checkbox"/> Sub Graduado <input type="checkbox"/> Graduado		_____
(7) Facultad, Escuela y Departamento u Oficina		(8)Teléfono de Contacto, Extensión o Núm. Celular:	
(9) Número de Serie de Tarjeta		Correo Electrónico: (10) Fecha expedición de la tarjeta	

(11) DESCRIPCIÓN DE ACCESOS CANCELADOS		
EDIFICIO	LUGAR QUE ABRIRÁ/OFICINA	HORARIO

(12) DESCRIPCIÓN DE CAMBIO (NUEVO ACCESO U HORARIO)		
EDIFICIO	LUGAR QUE ABRIRÁ/OFICINA	HORARIO

(13) DESCRIPCIÓN DE MOTIVOS:

Firma del Solicitante

Decano o Director de Departamento

Fecha

Fecha

INSTRUCCIONES GENERALES

Este formulario será completado en todas sus partes por el Administrador del Sistema de Acceso de la Unidad que otorga dicho acceso al usuario. El mismo deberá contar con la firma del Solicitante y el Decano, Director o su Representante (Administrador del Sistema de Acceso).

Instrucciones Específicas:

- (1) Nombre del Solicitante: se explica solo.
- (2) Identificación con foto: en el caso de empleados, marque si presentó licencia de conducir o tarjeta electoral; número de estudiante en el caso que el solicitante sea estudiante.
- (3) Dirección Residencial: lugar donde reside o se hospeda mientras estudia si es estudiante.
- (4) Dirección Postal (si diferente a la residencial): dirección en la que recibe la correspondencia.
- (5) Clasificación del Solicitante: indique si es visitante; empleado: docente, no docente; si es estudiante: graduado o sub graduado.
- (6) Término de Vigencia: indique el periodo que comprende la aprobación del acceso.
- (7) Facultad y Departamento u Oficina: Facultad y Departamento si es estudiante u Oficina a la cual pertenece el empleado.
- (8) Teléfono de Contacto y Correo Electrónico: Número de celular u hospedaje y dirección de correo electrónico actualizados
- (9) Número de Serie de Tarjeta: se explica solo
- (10) Fecha expedición de la tarjeta: fecha en que le fue otorgada la tarjeta de acceso.
- (11) Descripción de Accesos Cancelados: área de acceso controlado por tarjeta magnética para la cual le fue otorgado acceso.
- (12) Descripción de Cambio (Nuevo Acceso u Horario): Cambios en los accesos concedidos.
- (13) Descripción de Motivos: breve explicación de las razones para el cambio.



XI. CONTACTOS

UPRTP

José A. Rodríguez Vicenty
Decano Asociado
Decanato de Administración
787-764-0000 Ext. 84022
jose.rodriguez105@upr.edu



UPRTP

Samuel González González
Director
División de Seguridad y Manejo
de Riesgo (DSMR)
787-764-0000; Ext. 83764
samuel.gonzalez10@upr.edu



UPRTP

Carlos Ruiz Álvarez
Oficial de Seguridad IV
División de Seguridad y Manejo
de Riesgo (DSMR)
787-764-0000; Ext. 83768
carlos.ruiz9@upr.edu



UPRTP

Idalise Cuevas
Secretaria
División de Seguridad y Manejo
de Riesgo (DSMR)
787-764-0000; Ext. 83752
idalise.cuevas@upr.edu



UPRTP

Marilú Pérez Hernández
Decana Asociada
Decanato de Estudiantes
787-764-0000; Ext. 86097
marilu.perez1@upr.edu



UPRTP

Gloria Díaz Urbina
Decana
Decanato de Estudiantes
787-764-0000; Ext. 86003
gloria.diaz5@upr.edu



UPRTP

Darwin Marrero
Decano Auxiliar
Decanato de Servicios al Estudiante
787-764-0000; Ext. 86093
darwin.marrero@upr.edu



UPRTP

Lymari Barreto Feliciano
Directora
Oficina de Recursos Humanos
787-764-0000; Ext. 84413
lymari.barreto@upr.edu





UPRRP

Griselly Menéndez Rivera
Asistente de Administración III
Oficina de Recursos Humanos
787-764-0000; Ext. 84439
griselly.menendez@upr.edu



UPRRP

Brenda Hernández
Directora
Residencia ResiCampus
787-764-0000; Ext. 5645
brenda.hernandez@upr.edu



UPRRP

José Martínez Pérez
Asistente Administrativo
Residencia Torre Norte
787-764-0000; Ext. 86384
jose.martinez52@upr.edu



UPRRP

Alfredo Figueroa Llavat
Director
División de Tecnologías Académicas
y Administrativas (DTAA)
787-764-0000; Ext. 83801
alfredo.figueroa@upr.edu



UPRRP

Carlos Pereira
Decano Auxiliar
Decanato de Asuntos Administrativos
787-764-0000; Ext. 4747
carlos.pereira@upr.edu

