

Universidad de Puerto Rico

Oficina de Sistemas de Información

Administración Central



Guía de Seguridad para la Verificación de Identidad y Privacidad de los Datos Académicos en los Sistemas de Gestión de Aprendizaje Institucionales

Mayo 2023

Introducción

Los sistemas de gestión de aprendizaje institucionales se han convertido en una herramienta fundamental para la educación a distancia y presencial. Estos permiten a los estudiantes acceder a materiales de cursos, interactuar con los profesores y otros compañeros de clase, y realizar actividades de evaluación, todo desde una plataforma centralizada y en línea. A medida que aumenta el uso de estas plataformas, se vuelve cada vez más importante garantizar que la identidad de los estudiantes sea auténtica y segura. Además de garantizar la identidad de los estudiantes, es igualmente importante proteger sus datos personales y académicos.

Para lograr esto, los sistemas de gestión de aprendizaje deben contar con mecanismos de autenticación seguros que verifiquen la identidad de todos sus usuarios antes de permitir el acceso a la plataforma. Además, las plataformas de información deben implementar medidas de seguridad efectivas para proteger los datos de los estudiantes, incluyendo protocolos de seguridad que ayuden contra ataques malintencionados y accesos no autorizados.

Propósito

La Guía de Seguridad para la Verificación de Identidad y Privacidad de los Datos Académicos en los Sistemas de Gestión de Aprendizaje Institucionales tiene como propósito proporcionar principios y procedimientos generales sobre las medidas de seguridad necesarias para salvaguardar la integridad de los sistemas de gestión de aprendizaje institucionales, garantizando así la identidad de los estudiantes que acceden dichos recursos y proteger los datos personales y académicos de estos.

Alcance

Estas guías aplican a todos los Sistemas de Gestión de Aprendizaje (SGA) institucionales que sean utilizados para ofrecer cursos oficiales en cualquiera de las modalidades a distancia o como complemento a cursos presenciales. Aplica además a todos los usuarios que utilizan dichos sistemas como estudiantes, profesores, administradores o cualquier otro usuario con acceso otorgado por algún interés institucional.

Procedimiento

Como parte del proceso de admisión a nuestra institución, comienza un proceso de requerimiento de información que garantiza la identidad del estudiante. Durante el proceso se asigna una credencial institucional que le permite al estudiante acceder a los servicios de la Universidad de Puerto Rico. Una

parte esencial de esta credencial es el nombre de usuario, que además corresponde con el correo electrónico el cual es único, confidencial e intransferible. La información de identidad es replicada de forma integrada y segura entre los servicios de autenticación de la universidad.

En la Certificación 86 (2022-2023), las credenciales institucionales se categorizan como Datos Restrictos, lo que indica que son los datos más regulados y protegidos en la institución. Por lo tanto, es importante tratar las credenciales institucionales con el mayor nivel de seguridad y confidencialidad.

El Portal de la Universidad de Puerto Rico, <https://portal.upr.edu>, requiere que se provea información de seguridad y cambio de contraseña cuando un estudiante accede a la plataforma por primera vez. El proceso de cambio de contraseña exige unos requisitos para asegurar que la nueva contraseña tiene unas características de complejidad adecuado. Además, la información de seguridad provista es utilizada para verificación de identidad para cambios y recuperación de contraseñas.

Es responsabilidad del usuario manejar y asegurar responsablemente sus credenciales, tomando todas las precauciones necesarias de seguridad y confidencialidad. La credencial institucional identifica al individuo de forma única y es exclusiva para el uso de los servicios institucionales a los que se le brinda acceso.

El manejo de los expedientes académicos en los Sistemas de Gestión de Aprendizaje estará siempre en cumplimiento con los requisitos de las leyes locales y federales (Ej. *Family Educational Rights and Privacy Act* - FERPA). El acceso a los datos personales y académicos de los estudiantes estará restringido a los funcionarios que estén debidamente autorizados por la administración universitaria según establecido en las normativas institucionales.

El acceso a la información requiere el uso de credenciales institucionales validadas y accedidas por canales de comunicaciones seguros. Los controles de autorización en los Sistemas de Gestión de Aprendizaje de uso académico están establecidos según los récords de matriculación en el Sistema de Información Estudiantil Institucional. En la principal Plataforma de Gestión de Aprendizaje Institucional (online.upr.edu) la matriculación se hace de forma automática con el sistema estudiantil, manteniendo sincronizado los estudiantes y profesores con acceso a sus cursos.

La Universidad de Puerto Rico, a través de la Oficina de Sistemas de Información de Administración Central ha establecido una estrategia de seguridad institucional basada en la serie NIST (SP) 800 (Certificación 132 2021-2022). Esta estrategia se resume en (1) Infraestructura y Protección en Dispositivos, (2) Monitoreo y Respuesta, (3) Políticas, Reglamentos y Guías, y (4) Entrenamiento a los usuarios. Esta estrategia permite operar en un ambiente más seguro y en cumplimiento con las regulaciones estatales y federales.

En la actualidad, la Universidad de Puerto Rico no cobra cargos por la verificación de identidad del estudiante. En caso de cambios en este particular, es responsabilidad de la Universidad notificar previamente al estudiante.

Los Sistemas de Gestión de Aprendizaje de naturaleza académica cumplirán con las siguientes disposiciones relacionadas a la verificación de la identidad y la privacidad de los expedientes de los estudiantes.

1. Los estudiantes, profesores y administradores se autenticarán utilizando un servicio de inicio de sesión único (*Single Sign-on*) con sus credenciales institucionales (nombre de usuario y contraseña) según definido por la Oficina de Sistemas de Información de la Administración Central.

2. Se establecerán políticas de “contraseñas fuertes” que incluyan lo siguiente:
 - a. Longitud mínima de 8 caracteres
 - b. Longitud máxima de 16 caracteres
 - c. Combinación de caracteres especiales, números, letras mayúsculas y minúsculas.
3. Se implementarán protocolos de comunicación y acceso seguros para garantizar la protección de los datos y la autenticidad de los usuarios.
4. Se aplicarán oportunamente todas los parchos y actualizaciones de seguridad disponibles.
5. Se orientará a los usuarios en temas de seguridad para ayudarles a comprender la importancia de mantener sus credenciales de inicio de sesión seguras y proteger su información personal (itsecurity.upr.edu).
6. Se harán accesibles opciones de navegadores seguros y/o sistemas especializados para el acceso a exámenes en línea.
7. Los sistemas que albergan estas plataformas cumplirán con la [Guía de Configuración de Servicios Electrónicos](#) (www.upr.edu/itdocs) de la Oficina de Sistemas de Información de la Administración Central y otras guías y procedimientos aplicables.
8. Se restringirá el acceso a los cursos oficiales a funcionarios autorizados, profesores que lo ofrecen, los estudiantes matriculados en este y usuarios con acuerdos regulados, como estudiantes oyentes, asistentes de cátedra, entre otros.

Esta guía ha sido revisada y aprobada por la Oficina de Sistemas de Información de la Administración Central en colaboración y acuerdo con la Vicepresidencia de Programas Profesionales y Educación a Distancia de la Universidad de Puerto Rico.