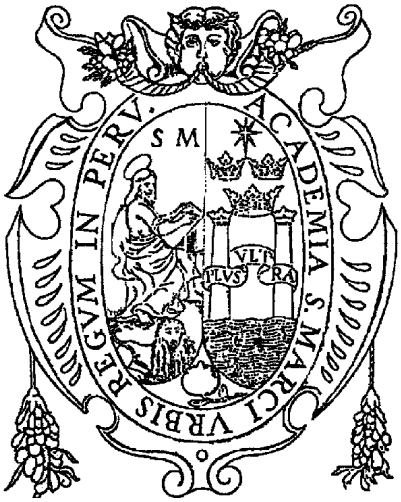
Universidad Nacional Mayor de San Marcos
Facultad de Ingeniería de Sistemas e Informática
E.P. de Ingeniería de Software



PEP-DAGIA: Arquitectura de gestión de identidades y accesos

Integrantes

Calle Huamantinco, Luis Eduardo	22200255
Calongos Jara, Leonid	22200102
Flores Cóngora, Paolo Luis	22200232
Pariona Molina, Matthew Alexandre	22200235
Calderón Matias, Diego Alonso	22200074
Luján Vila, Frank José	12200058

Curso: Gestión de la Configuración del Software.
Docente: Wong Portillo, Lenis Rossi.

PEP-AGIA: Arquitectura de gestión de identidades y accesos

1. Autenticación

El sistema de gestión de identidades y accesos utilizará un **sistema de autenticación basado en roles** para los tres tipos de usuarios, gestionando los permisos de cada uno en función de su identidad y rol asignado. La autenticación será exclusiva para los estudiantes de la Facultad de Ingeniería de Sistemas e Informática (FISI) de la Universidad Nacional Mayor de San Marcos (UNMSM).

- **Métodos de autenticación**:
  - **OAuth 2.0 o JWT (JSON Web Tokens)**: Los usuarios inician sesión utilizando sus credenciales proporcionadas por el sistema central de autenticación de la universidad. El sistema verificará la identidad utilizando OAuth 2.0 o a través de JWT para asegurar el acceso.
  - **Doble factor de autenticación (2FA)**: Se implementará para los administradores generales y opcionalmente para los usuarios, utilizando métodos como correo electrónico o autenticadores de dispositivos móviles.

2. Identidades de usuario

El sistema utilizará una **base de datos centralizada** para almacenar los datos de los usuarios, incluyendo su perfil, historial de actividad, y roles asignados. Los tres roles clave son:

- **Admin general**: Tiene acceso total a la plataforma, incluyendo la gestión de foros y usuarios, la moderación de comentarios y la administración de notificaciones.
- **Usuario creador de foros**: Puede crear y gestionar sus propios foros. Puede invitar a otros usuarios a comentar y gestionar las discusiones.
- **Usuario participante**: Puede comentar y participar en discusiones en los foros creados por otros usuarios, además de poder calificar a los profesores.

3. Autorización y Control de Acceso

El sistema IAM gestionará los permisos y accesos utilizando un **modelo basado en roles (RBAC)**. Cada rol tiene permisos específicos dentro del sistema, y las restricciones se basan en el tipo de usuario:

- **Admin General**:
  - Crear, modificar y eliminar foros.
  - Moderar comentarios y calificaciones.
  - Gestionar usuarios.
  - Configurar notificaciones automáticas.
- **Usuario Creador de Foros**:

    - Crear y administrar foros personales.
    - Editar y eliminar sus propios foros.
    - Invitar a otros usuarios a comentar.
- **Usuario Participante**:
    - Comentar y calificar en los foros creados por otros usuarios.
    - Participar en discusiones y responder a otros comentarios.

Cada acción dentro de la plataforma será evaluada por el sistema IAM para verificar si el usuario tiene los permisos adecuados antes de conceder acceso.

4. Gestión de Sesiones

El sistema debe mantener sesiones seguras para cada usuario, con la opción de cerrar sesión manualmente o por expiración automática tras un periodo de inactividad. Las sesiones serán gestionadas mediante cookies seguras y tokens de acceso que se regenerarán periódicamente para evitar el secuestro de sesiones.

5. Auditoría y Registros de Actividad

El sistema incluirá una función de **auditoría y monitoreo**, registrando todas las actividades críticas de los usuarios, como:

- Creación y eliminación de foros.
- Modificación de comentarios o calificaciones.
- Inicio y cierre de sesión.

6. Seguridad y Protección de Datos

La arquitectura IAM incluirá **mecanismos de seguridad** para proteger las identidades y los datos de los usuarios:

- **Cifrado**: Todos los datos sensibles, como contraseñas y tokens, se almacenarán cifrados utilizando algoritmos modernos de cifrado, como AES-256.
- **Protección contra ataques**: La plataforma estará protegida contra ataques de inyección SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), y otros tipos de vulnerabilidades comunes.
- **Política de contraseñas**: Se aplicará una política de contraseñas fuertes, que incluye la verificación de la fortaleza de las contraseñas y la caducidad periódica de las mismas para los administradores.