

Seguridad en Redes y Datos



Identity and Access Management

Tormenta de Ideas



- * ¿Qué entendemos por IAM?
 - * Gestión de usuarios (permisos entre otros)
 - * Quien puede hacer qué en donde
 - ★ El lugar donde un usuario se loguea y donde revisamos si tiene el permiso para acceder
 ★ ¿Ej. AD?
 - * Políticas de seguridad que tengan que ver con usaurios
 - 🗶 🛮 Integrado con auditoría

Tormenta de ideas



- * ¿Qué elementos componen IAM?
 - * Políticas
 - * Usuarios
 - ***** Grupos
 - ⋆ OUs
 - * Privilegios/Permisos
 - * Roles
 - ⋆ Group Policy
 - * Recursos/Objetos

¿Qué es IAM?



- * Identity:
 - * Relación entre una identidad real y su representación digital
 - Normalmente representada por un usuario y su contraseña
 - ¿Otras representaciones?
- * Access:
 - Permisos de acceso a recursos e información
 - * Normalmente lo vemos como listas de permisos
 - * ¿Otras formas de modelarlo?
- Management:
 - * Gestión de lo anterior
 - Procesos, productos y políticas que nos permitan manejarlo

Componentes de IAM



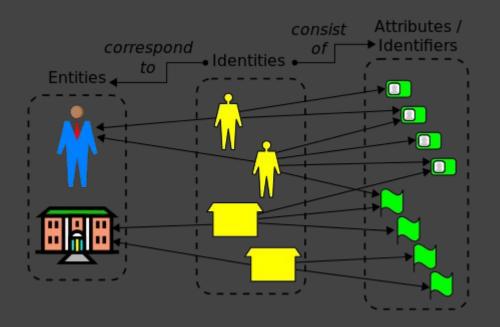


Tipos de Identidad



- Usuario/contraseña
- * Token
- Certificado digital
- Dirección IP u otra forma de direccionamiento

 Cualquier conjunto de atributos que nos permitan determinar unívocamente una entidad



Ciclo de vida de la identidad



Provisioning

- Create person and identifiers (GID and PIDM in Banner)
- Define his/her group and role membership (Faculty, Staff, Student)
- Accounts created with pickNetID platform
- Stand alone accounts provisioned for Banner, Argos, BDM, etc.
- Guest and shared accounts are created via authorized forms.
- Flex-Reg (Pace)

Authentication

- Validate the person's identity
- Typically NetID and Password
- Local Authentication

Identity Vetting

- Undergraduate admissions
- Graduate admissions
- International Students and Scholars
- **Employment identity**
- Professional and Continuing Education
- **Guests accounts**
- Faculty that are granted emeritus status
- Full details on Identity vetting below:
- https://docs.google.com/document/d/18dasD m-xwdqZpnfcWHhqqqtCVzSiOBqU-D7KbU9j 1EY/edit?usprsharing

Identity Lifecycle

Identity and Access Management (IAM) is the set of business policies, processes, and a supporting infrastructure for managing the creation, maintenance and use of digital identities.

IAM enables organizations to:

- Provide secure access to resources
- Efficiently control this access
- Respond faster to changing relationships
- Protect confidential information from unauthorized users
- Verifies your Identity
- Manages what you can and cannot do based on business rules and your attributes such as departmental affiliation. or role within the university
- Limited to accounts owned by users or groups, this does not include system or service level accounts

De-provisioning

- Revoking permissions/access
- Removing LDAP, Google and AD accounts.
- Revoking Argos, Banner, BDM access, etc.
- NetID Accounts Expiration for faculty, staff, students, guest, etc.
- https://www.oakland.edu/uts/common-good-core-resources/accounts/#netid

Self-Service

- NetID Password and resets
- **GID Pin resets**
- Preferred Name changes
- Maintenance of person information (core person attributes)
- Replication of person attributes to other systems as required (Banner, LDAP, Google and AD)

Authorization

- Determine rights to a system
- Audit and security reporting
- Manage access to systems

- Determine access rights
- Manage user permissions
- Host access and sudo access

Permissions

Implementaciones



- User/Pass
- * LDAP
- * AD
- * Kerberos
- * PKI
- * ¿Radius?

Roles y gestión de grupos de identidad (¿Recuerdan RBAC?)

Productos



- * Thycotic
- Centrify
- Windows Active Directory
- * OpenLDAP
- OpenIAM

Desafíos



- * Integración
 - * Termina definiendo la solución
- * Costo de implantación
 - * Puede ser difícil llegar a relevar y normalizar todos los permisos
- Gestión de usuarios privilegiados
 - * No siempre puedo prescindir de los Administrator o root

Implementaciones complejas



- * Autenticación Federada
- * OAuth