Construyendo una Arquitectura de Gestión de Identidades para PS

Building an Identity Management Architecture for PS

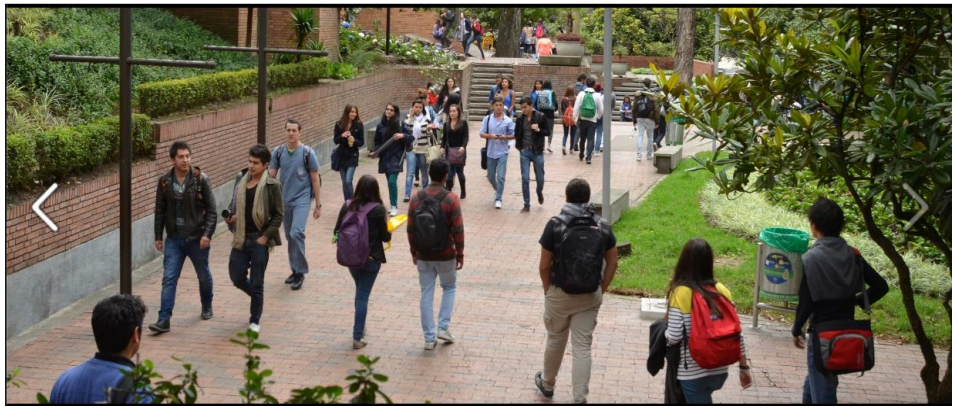
PONTIFICIA UNIVERSIDAD JAVERIANA

Colombia – Bogotá

Agosto 23 de 2016

Agenda propuesta

Pontificia Universidad Javeriana - Colombia



Pontificia Universidad Javeriana - Colombia

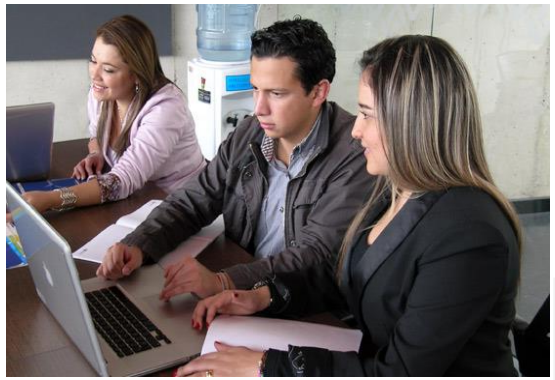
190 estudiantes de doctorado

1.881 estudiantes de maestría

1.822 estudiantes de especialización

18.995 estudiantes pregrado

1.266 profesores planta



1.996 profesores cátedra

1.568 personas planta administrativa

Productos de Oracle en la PUJ

DB 12 con soporte en 11

HCM 8.52: campus, HR, e-performance, …
FN 8.52: KK, GL, AP, …
EP 8.49

OUD 11R2
OIM 11R2 sin SP
OAM 11R2 SP3

BI – Exalitics
Administrativo
Estudiantes early adopters 38i
Profesores OBIEE 30i

Hyperion

CRM elocua, rightnow

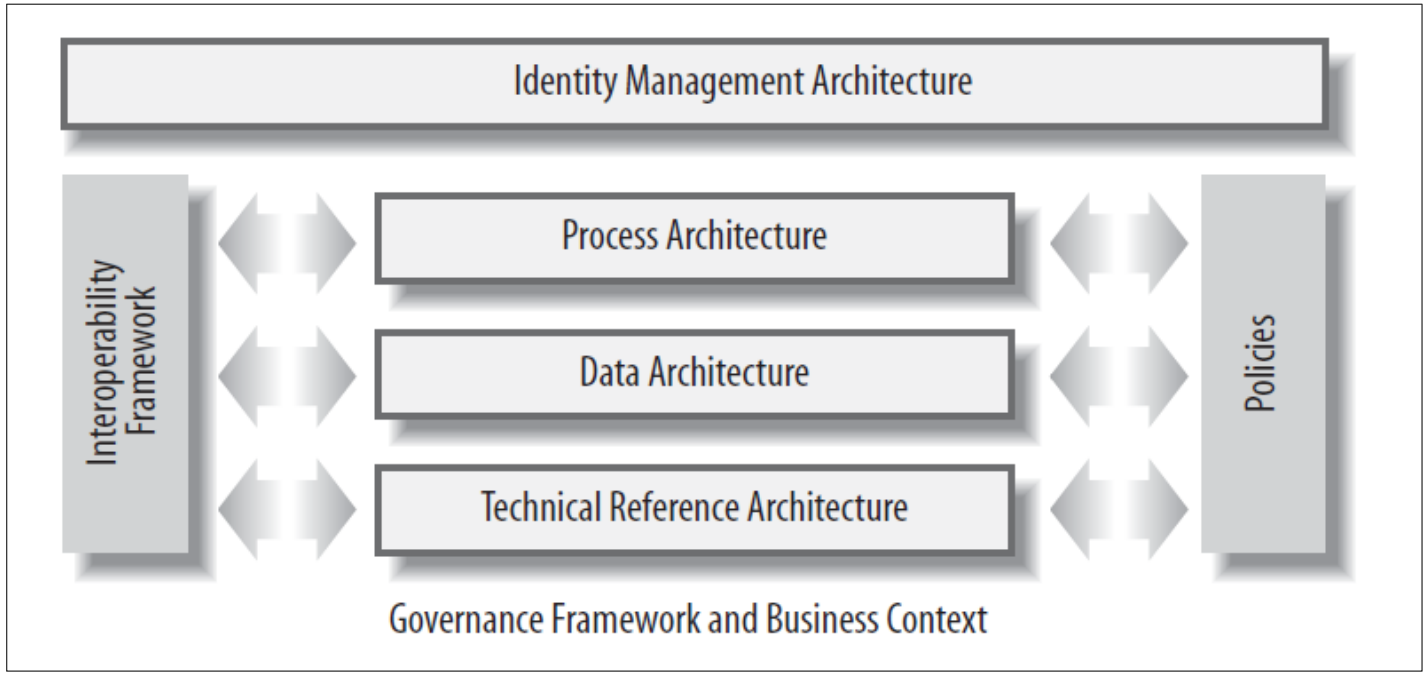
Gestión de Identidades y de Accesos

'IAM es la disciplina de la seguridad que habilita a los ***individuos*** *correctos a acceder a los* ***recursos*** *correctos en los* ***momentos*** *correctos y por las* ***razones*** *correctas.*

IAM direcciona las necesidades de mission critica, de asegurar el apropiado acceso a recursos a través de los ***ambientes tecnológicos incrementalmente hetereogeneos****, y de alcanzar los* ***requerimientos incrementalmente rigurosos de cumplimiento****. Esta práctica de seguridad es un emprendimiento crucial para cualquier organización. Debe estar incrementalmente alineada con la organización, requiriendo de* ***perfiles en negocio y no solo experiencia técnica****.*

Las organizaciones que desarrollan capacidades maduras en IAM pueden reducir sus costos de gestión de identidad y mas importante se vuelven significativamente ***mas ágiles en soportar las nuevas iniciativas de la organizacion.' Gartner***

Gestión de Identidades y de Accesos

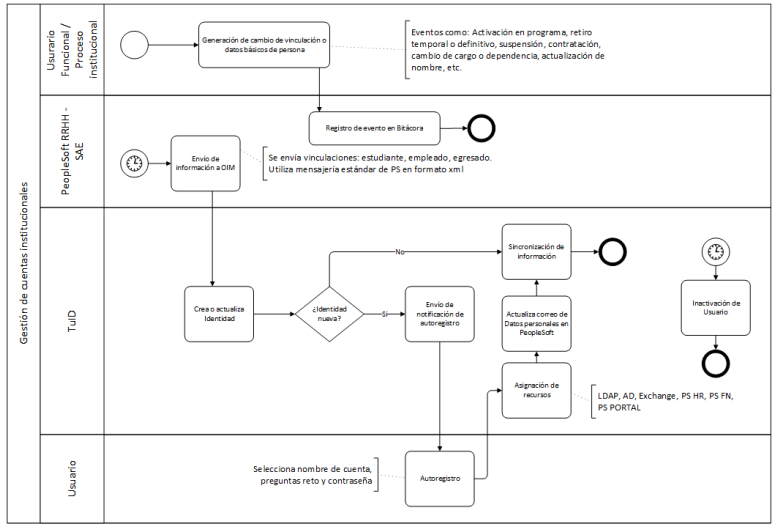


Digital Identity, Phillip J. Windley

Gestión de Identidades y de Accesos

Pre

- Levantamiento de procesos funcionales,
- *Benchmarking*,
- ***Single Login:*** directorios, múltiples sistemas, fuentes de autenticación,
- Políticas: cuenta única por persona y múltiples atributos
- POC
- Proyecto de implementación!



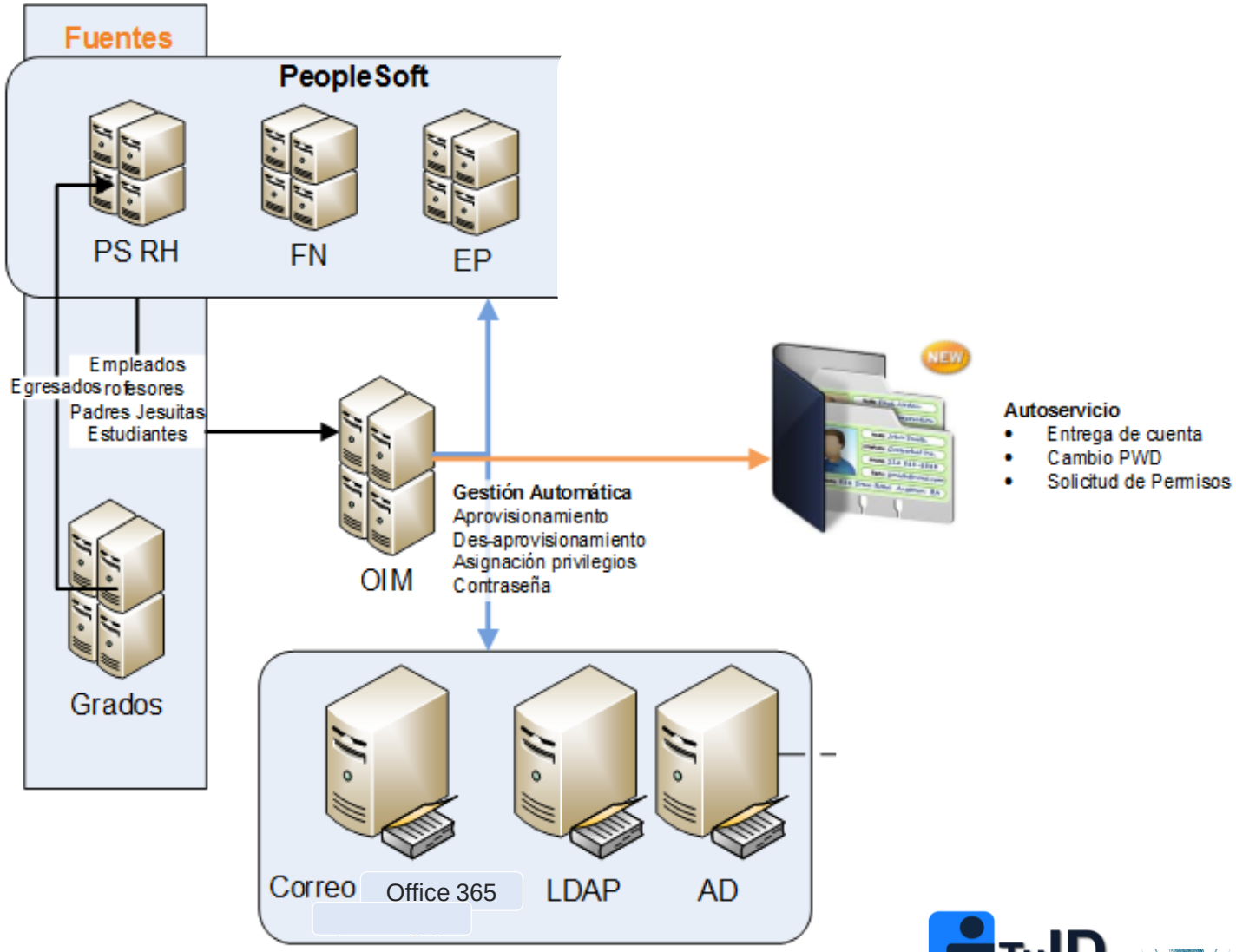
2012 2013 2014 2015 2016

Gestión de Identidades

TuID es el sistema que permite gestionar las cuentas de usuario y sus accesos, de acuerdo a las vinculaciones de la persona con la Universidad.

- Manejo de ciclo de identidad, creación (aprovisionamiento), actualización e inactivación (des aprovisionamiento),
- Entrega de cuenta – Autoregistro,
- Autoservicio de contraseñas: cambio y recuperación con preguntas reto,
- Solicitud de permisos adicionales sobre Peoplesoft.
- Cambio de directorio de OpenLDAP por OUD

Gestión de Identidades – Arq Tech



Gestión de Identidades - Alcance

Padre Jesuita

Empleado Administrativo o Académico

Profesor
- Planta
- Cátedra

Estudiante

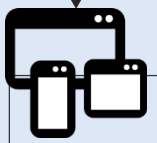
Egresado

Privilegios Generales

Correo Electrónico

PeopleSoft (HR, Fn, Portal)

Directorios AD, LDAP



Otros servicios

- Red Inalámbrica
- BD Biblioteca
- Acceso a BlackBoard
- Etc.

- El sistema responde a procesos funcionales como: matricula de estudiante, retiro temporal o definitivo, contratación, terminación de contrato, etc.
- TuID gestiona datos como: nombre, documento, dependencia, programa académico, fechas de contrato, etc.
- La fuente de información de TuID es nuestro ERP PeopleSoft.
- La información enviada a los diferentes sistemas y/o servicios corresponde a lo registrado en PeopleSoft.
  - Ej: Agenda Outlook -> Nombres
- No es posible generar excepciones.
  - Ej: Nombres -> se extrae de PS.

TuID · Pontificia Universidad Javeriana Bogotá · Latin America · HEUG

Gestión de Identidades - Jerarquía

Caso 1: Privilegios excluyentes
Ej: política de vencimiento de contraseña

Se aplica jerarquía

Caso 2: Privilegios NO excluyentes
Ej: Acceso a ERP PeopleSoft.

Se suman privilegios

Gestión de Identidades – Ejemplo

Padre Jesuita

Empleado Administrativo o Académico

Profesor
- Planta
- Cátedra

Estudiante

Egresado

- Plataforma de correo ~~**Exchange**~~ **Office 365**
- Prima para la **información de contactos** Outlook
- Vigencia de cuenta **periodo de contrato**
- Cambio de contraseña: **60 días**
- Al finalizar contrato se inactiva la cuenta
  - Si existen otras vinculaciones se asigna **otra cuenta**
    - c.camargo01@javeriana.edu.co
- Empleado académico = Privilegios de Profesor

Gestión de Identidades – Ejemplo

Padre Jesuita

Empleado Administrativo o Académico

Profesor

- Planta
- Cátedra

Estudiante

Egresado

- Plataformas de correo **Office 365**
- Vigencia **fin contrato + 365 días**
- En caso de **otras vinculaciones se mantiene la** cuenta
- Profesores **ad honorem** cumplen este esquema.

Gestión de Identidades – Ejemplo

Padre Jesuita

Empleado Administrativo o Académico

Profesor
- Planta
- Cátedra

Estudiante

Egresado

- Plataformas de correo **Office 365**
- Vigencia **retiro temporal o retiro definitivo + 2 años**
- En caso de **otras vinculaciones se mantiene la** cuenta
- Estudiantes **ALE** tiene **6 meses** de vigencia posterior a la terminación.

Gestión de Identidades – Ejemplo

Padre Jesuita

Empleado Administrativo o Académico

Profesor
- Planta
- Cátedra

Estudiante

Egresado

- Plataformas de correo **Office 365**
- Vigencia **indefinida**

Gestión de Identidades – Ejemplo

Padre Jesuita

Empleado Administrativo o Académico

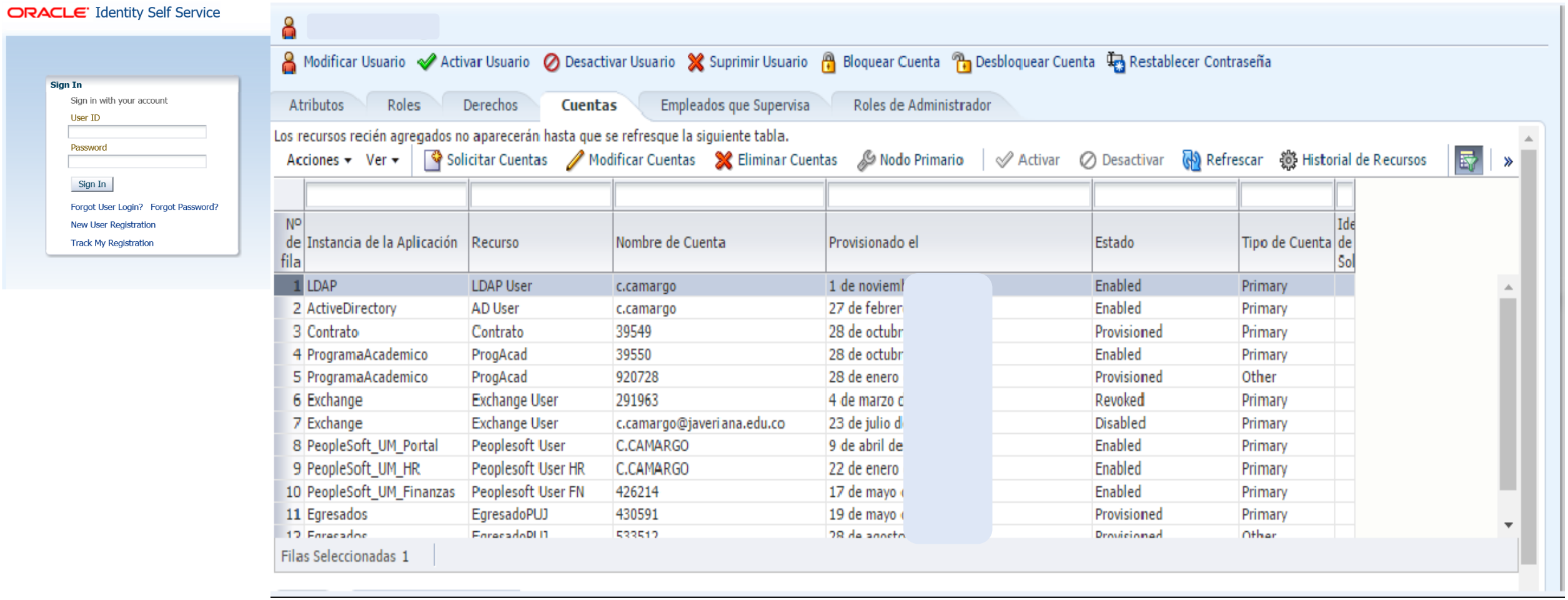
Profesor
- Planta
- Cátedra

Estudiante

Egresado

- Plataformas de correo ~~**Exchange**~~ **Office 365**
- Vigencia indefinida
- Aplican políticas de acuerdo a otras vinculaciones

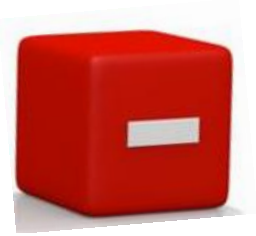
Gestión de Identidades – Ejemplo



Gestión de Identidades - Impactos

- Automatización de entrega de cuentas.
  - No intervención de facultades.
- Autogestión.
  - Selección de nombre cuenta.
  - Asignación de contraseña.
  - Preguntas reto.
- Centralización en asignación de recursos TI.
- Creación Perfiles de Usuario PS en el registro.
  - Reducción de mensajería PS.

- Inconvenientes en activación.
- Casos de no envio automático de correo de autoregistro.
- Nuevos perfiles de PS sin email.
  Cargue de cuentas a BlackBoard



Gestión de Identidades - Retos

- Calidad de datos: correo alterno, fecha de nacimiento, fecha de expedición de documento de identidad, teléfono y dirección.
  - Causa 1: controles de datos obligatorios de PERSONAL_DATA.
  - Causa 2: En el formulario de admisión la fecha de nacimiento permite ingresar la fecha actual.
    - Solución: Incluir control de fecha de nacimiento > 10 años , encargado OSI; <requerimiento>.
  - Causa 3: Encargados de Admisión Rápida no ingresan información correcta. Posible desconocimiento.
  - Causa 4: Gestión de Identidades y de Accesos - Impactos

Gestión de Identidades - Retos

- PeopleSoft no esta reportando a OIM algunos eventos.
  - Causa 1: Bug en PS, los cambios por Admisión rápida de estudiantes no se informan a OIM. ALE: Movilidad nacional, internacional, convenio sígueme, conexión javeriana, PREU, etc.
  - Causa 2: Actualización de documento de identidad no se reporta
- Errores de acceso a PeopleSoft
  - Causa 1: Estudiantes o personal antiguo que nunca habían entrado a PeopleSoft no tenían cuenta; OIM asigna recursos a los nuevos usuarios. Caso postgrados.
- Incidentes asociados a Formulario de admisión.
  - Causa 1: Actualmente para usuarios que tuvieron alguna vinculación se requiere autenticación. Implica reactivar cuentas de usuario inactivas.
  - Causa 2: Un usuario que cambió de documento y se registra a un nuevo programa genera una persona duplicada en PS.

Gestión de Identidades - Retos

Operación

- Mejorar mecanismo de sincronización (Validación) periodos pico por alto número de cambios eje: Semana de matrículas.
- Generar mecanismos para delegar a la mesa de servicio las tareas de envío de correo y sincronización (validación) manual.
- Proceso de asignación de correo electrónico en el perfil de usuario de PeopleSoft para cuentas nuevas.

Gestión de Identidades- Retos

Operación

- Revisión de JMS y *tunning*. casos:
  - Demora en sincronización de contraseña.
  - Demora en sincronización de documento de identidad y en ocasiones no se actualiza la información.
- Resolver inconsistencias y carga de usuarios:
  - Se requiere reconciliar recursos y completarles lo que les haga falta a Egresados, estudiantes, empleados y profesores que se reincorporan.
  - Desconocimiento del proceso por parte de directores de programa, indicaciones en impresión de facturas

Gestión de Identidades - Retos

Restauración de contraseña

- Las preguntas y respuesta reto: SON UN RETO!!

Gestión de Identidades - Retos

Asignación de permisos.

- Por poblaciones, por cargos,
- Pero la asignación de permisos de funciones no fácilmente identificables por cargo y delegaciones.
- UX mejorada con un módulo de gestión de flujos.

Gestión de Accesos

Unificar el acceso,

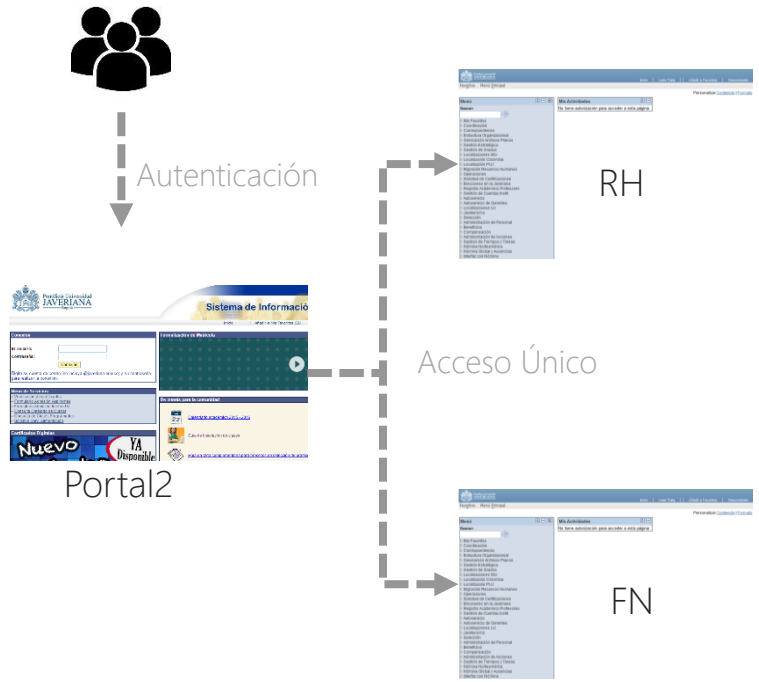
Facilitar el uso minimizando el número de *logins*,

Portal de aplicaciones,

Gestión de Accesos – Fase 1

Gestión de Accesos – F2 - Arquitectura Técnica

Situación Actual



Objetivo

Gestión de Accesos – F2 - Retos

- Autenticación de administradores
- Autenticación de la otra sede – usando otro directorio
- Disponibilidad
- Pruebas de carga

Gestión de Identidades y Accesos

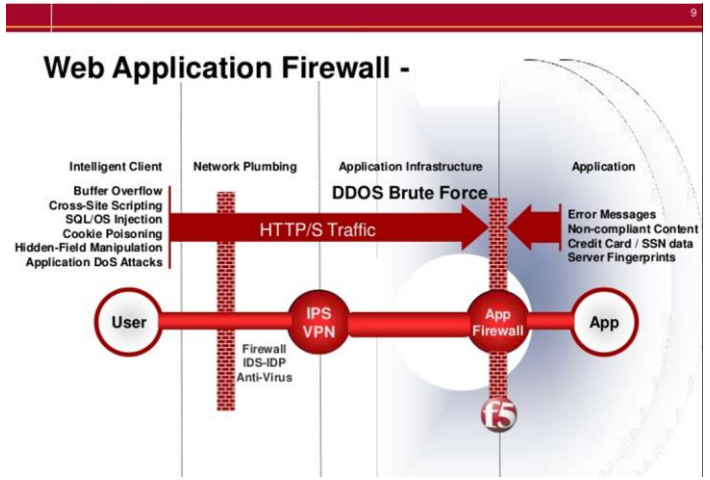
- OUD,
- OIM,
- OAM,
- asignación dinámicas en PS,
- por atributos y grupos en LDAP – AD: BI, Hyperion,… otras aplicaciones
- Flujos de solicitud - manual,

Seguridad en PS

Asignación de roles es suficiente?

DAM:

- 1521/tcp sobre algunas bases de datos HR, FN, EP,
- SO de los servidores del RAC
- Monitoreo de transacciones Sensibles: administradores de DB, de usuarios, datos personales y notas
- Operaciones privilegiadas sobre la DB: alter
- Alertas en cambios de cargo y retiro de roles automáticos
- User tracking el usuario login en peoplesoft



WAF:

- Protección de FW para PS y WWW
- Seguridad positiva, Seguridad negativa
- firmas para PS y manipulación de parámetros y de URLs, DDoS, Brute Force,
- Parámetros privilegiados gestión de estos parámetros Dinámicos, no se manipulan del cliente,
- User tracking para saber el usuario quien intenta,
- No se pudo web scrapping

Seguridad en PS

Asignación de roles es suficiente?

- Auditorias,: hallazgos componentes, parámetros de configuración de cuentas – sintaxis, *timer-out*.
- Gestión de proyectos TI - SEGURO
- *Ethical Hacking*: sobre el modulo de gestión de notas
- Seguridad Perimetral
- Concientización

Gestión de Identidad – Próximos pasos

- Migración a 9.2,
- Autenticación de doble factor,
- Calidad de Datos: gobierno y arquitectura de datos, requerimientos de la Dirección de Impuestos Nacionales, duplicidad de identidades, Ministerio del Exterior,
- Datos Personales: cumplimiento con la ley de protección de datos personales – 1581 de 2012 -reporte de bases de datos.
- EH: práctica permanente para components actuales y paso de proyectos PS futuros.

Referencias

- Garnet IAM definition: http://www.gartner.com/it-glossary/identity-and-access-management-iam/
- ISO/IEC 24760-1:2011 Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts
- Phillip J. Windley Digital Identity O'Reilly, 2005

¡Gracias!

Nelson Gómez
Jefe de Seguridad Informática
Pontifica Universidad Javeriana
ngomez@javeriana.edu.co