

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

OULD 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

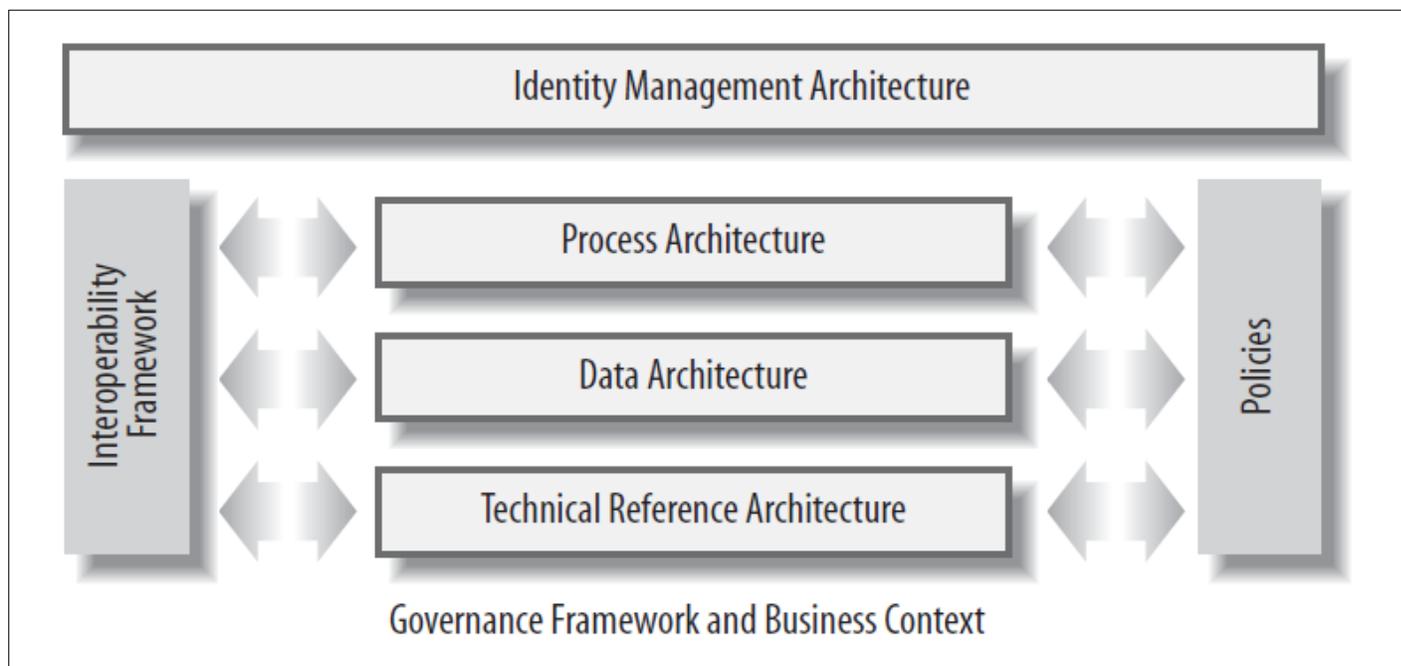
*'IAM es la disciplina de la seguridad que habilita a los **individuos** correctos a acceder a los **recursos** correctos en los **momentos** correctos y por las **razones** correctas.*

*IAM direcciona las necesidades de misión crítica, de asegurar el apropiado acceso a recursos a través de los **ambientes tecnológicos incrementalmente heterogéneos**, 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 más importante se vuelven significativamente **mas ágiles** en soportar las nuevas iniciativas de la organización.' Gartner*



Gestión de Identidades y de Accesos



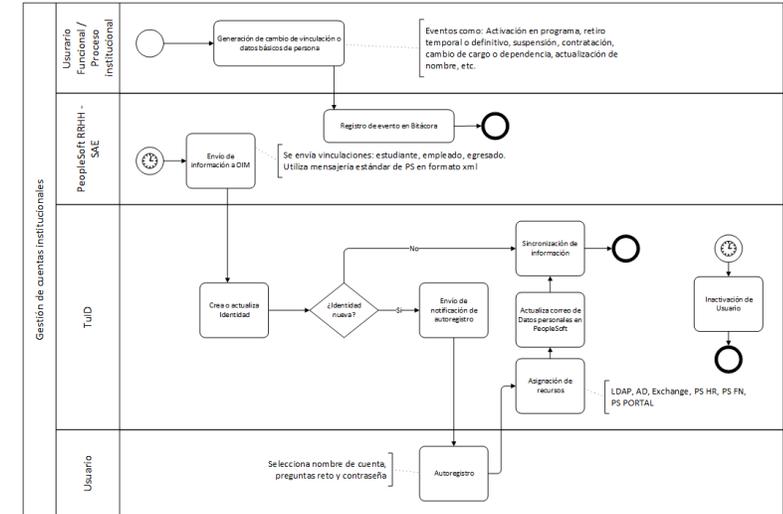
Digital Identity, Phillip J. Windley



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!



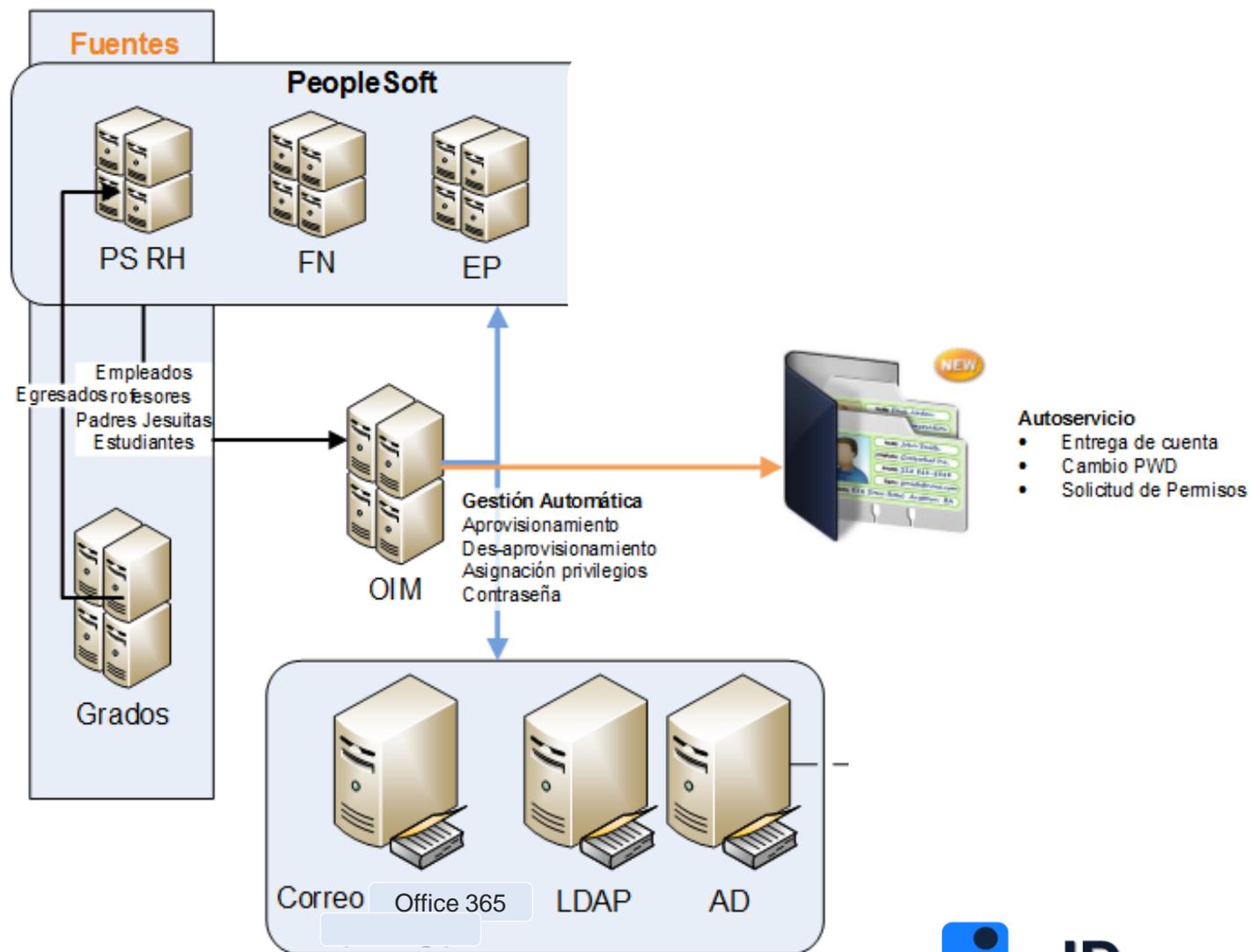
Gestión de Identidades

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 (desaprovisionamiento),
- 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

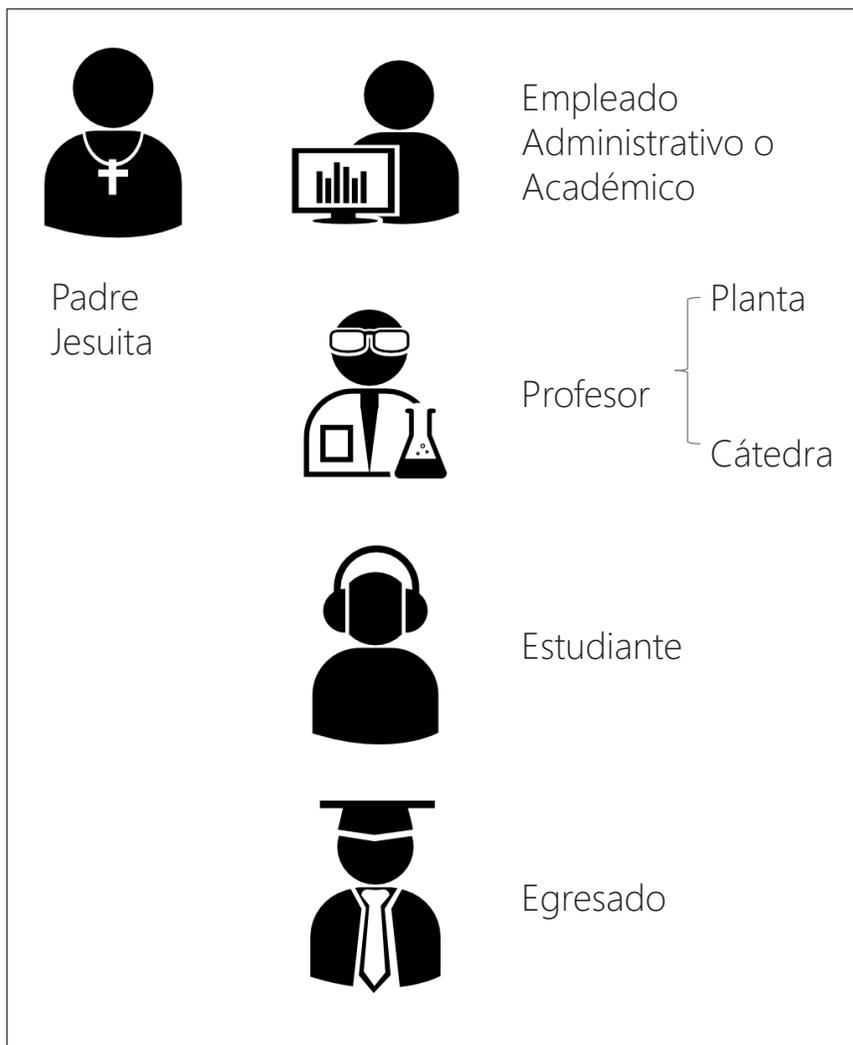


Gestión de Identidades - Alcance



- 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.

Gestión de Identidades - Jerarquía



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



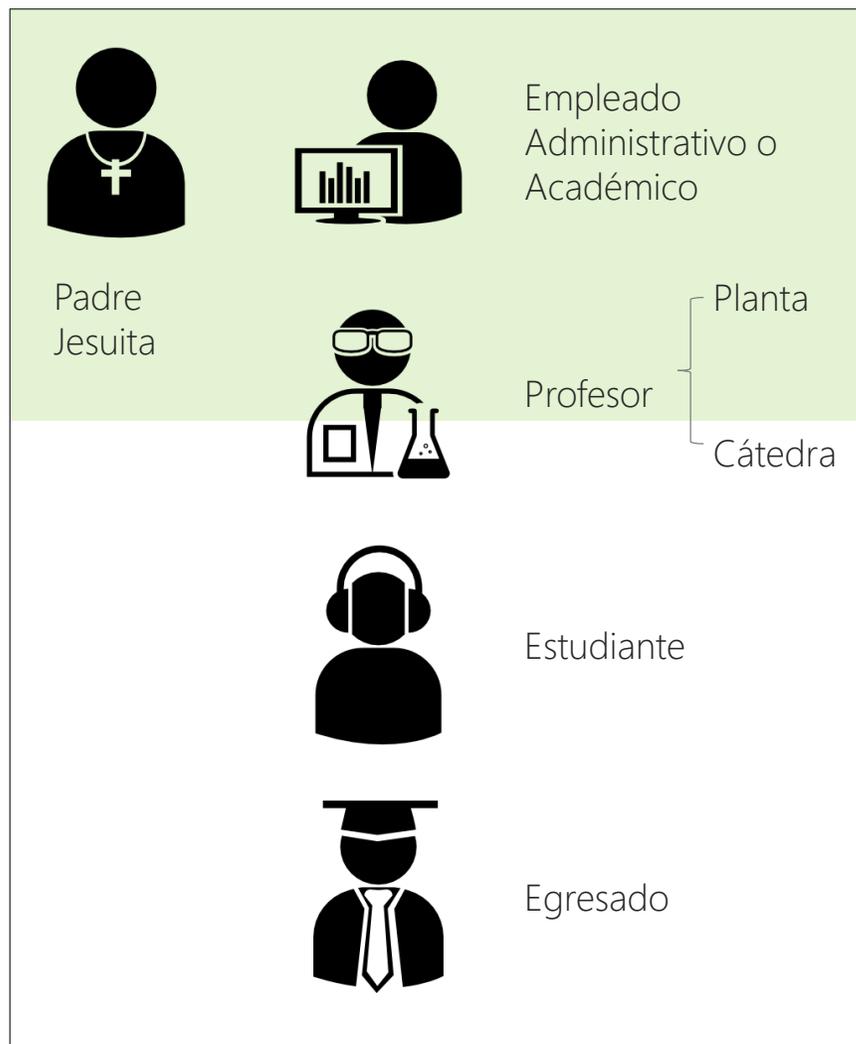
Se aplica jerarquía

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



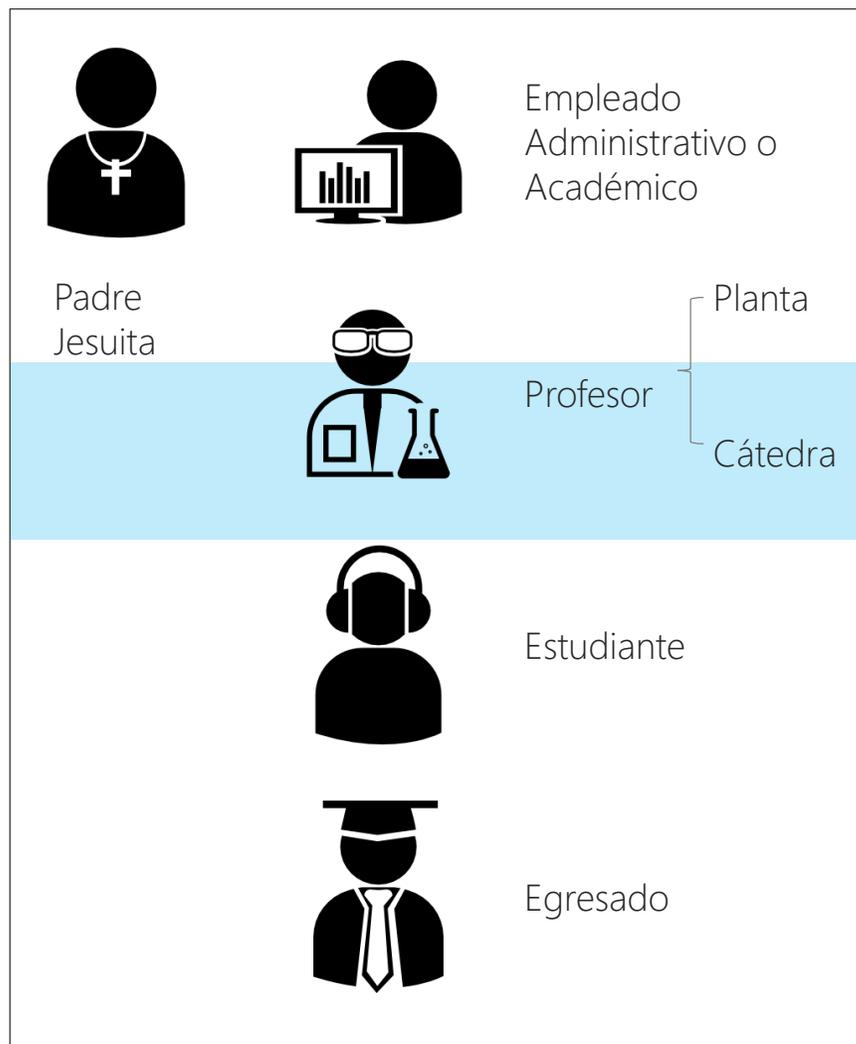
Se suman privilegios

Gestión de Identidades – Ejemplo



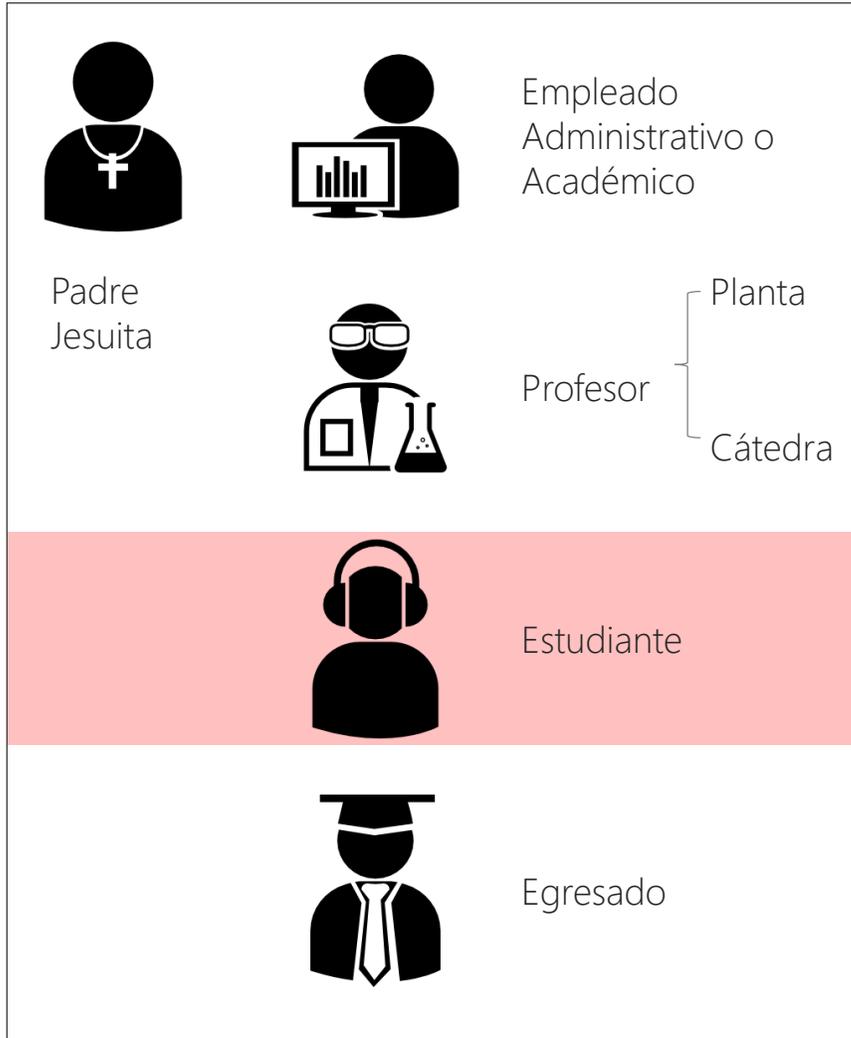
- Plataforma de correo **Exchange Office 365**
- Prima para la **información de contactos** Outlook
- Vigencia de cuenta **periodo de contrato**
- Cambio de contraseña: **60 días**
- Al finalizar contrato se inactiva la cuenta
 - Si existen otras vinculaciones se asigna **otra cuenta**
 - c.camargo01@javeriana.edu.co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

Gestión de Identidades – Ejemplo



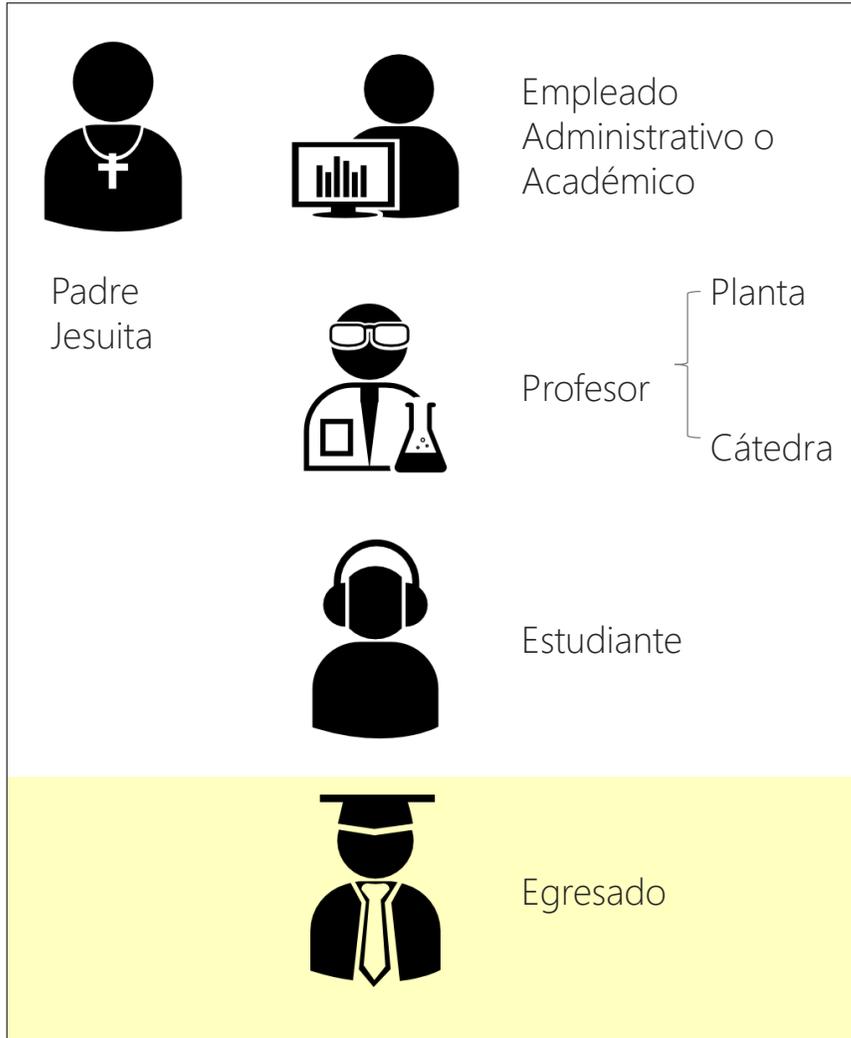
- Plataformas de correo **Office 365**
- Vigencia **fin contrato + 365 días**
- En caso de **otras vinculaciones se mantiene la cuenta**
- Profesores **ad honorem** cumplen este esquema.

Gestión de Identidades – Ejemplo



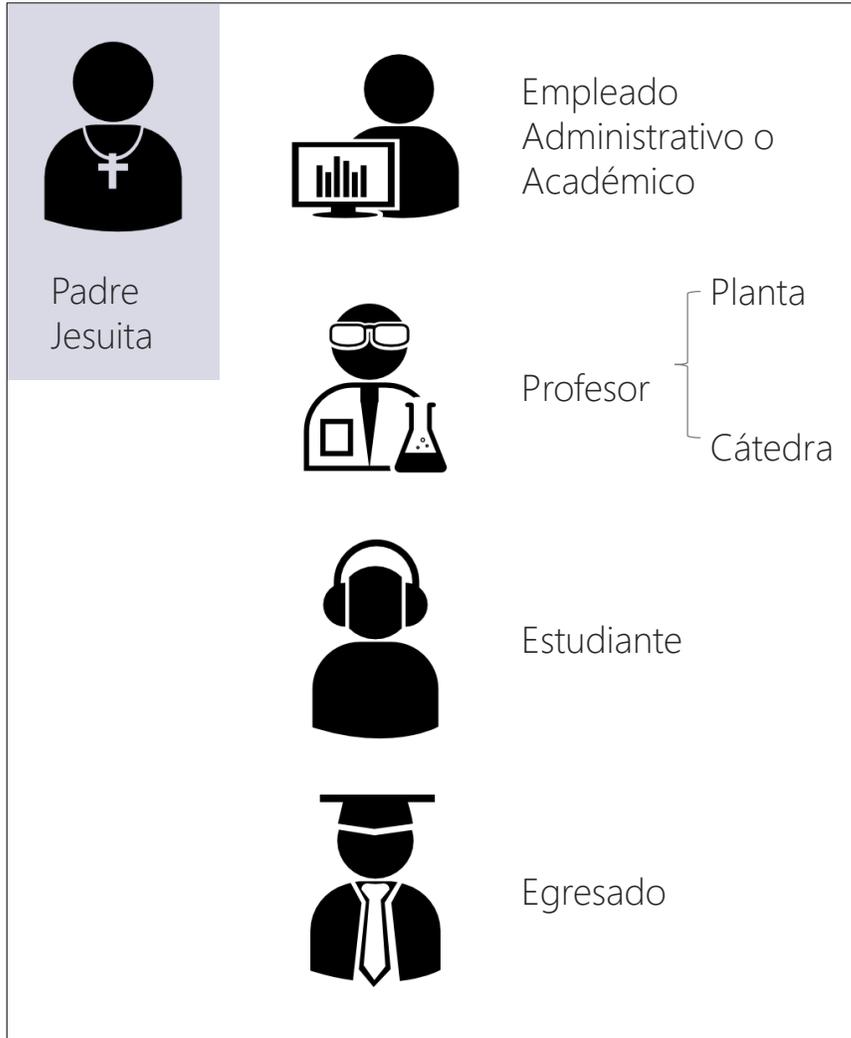
- Plataformas de correo **Office 365**
- Vigencia **retiro temporal o retiro definitivo + 2 años**
- En caso de **otras vinculaciones se mantiene la cuenta**
- Estudiantes **ALE** tiene **6 meses** de vigencia posterior a la terminación.

Gestión de Identidades – Ejemplo



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

Gestión de Identidades – Ejemplo



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

Gestión de Identidades – Ejemplo

ORACLE Identity Self Service

Sign In

Sign in with your account

User ID

Password

Sign In

[Forgot User Login?](#) [Forgot Password?](#)

[New User Registration](#)

[Track My Registration](#)

Modificar Usuario ✓ Activar Usuario ⊘ Desactivar Usuario ✗ Suprimir Usuario 🔒 Bloquear Cuenta 🔓 Desbloquear Cuenta 🔄 Restablecer Contraseña

Atributos
Roles
Derechos
Cuentas
Empleados que Supervisa
Roles de Administrador

Los recursos recién agregados no aparecerán hasta que se refresque la siguiente tabla.

Acciones ▾ Ver ▾
 Solicitar Cuentas
 Modificar Cuentas
 Eliminar Cuentas
 Nodo Primario
 Activar
 Desactivar
 Refrescar
 Historial de Recursos

Nº de fila	Instancia de la Aplicación	Recurso	Nombre de Cuenta	Provisionado el	Estado	Tipo de Cuenta	Ide de Sol
1	LDAP	LDAP User	c.camargo	1 de noviem/	Enabled	Primary	
2	ActiveDirectory	AD User	c.camargo	27 de febrer	Enabled	Primary	
3	Contrato	Contrato	39549	28 de octubr	Provisioned	Primary	
4	ProgramaAcademico	ProgAcad	39550	28 de octubr	Enabled	Primary	
5	ProgramaAcademico	ProgAcad	920728	28 de enero	Provisioned	Other	
6	Exchange	Exchange User	291963	4 de marzo d	Revoked	Primary	
7	Exchange	Exchange User	c.camargo@javeriana.edu.co	23 de julio d	Disabled	Primary	
8	PeopleSoft_UM_Portal	Peoplesoft User	C.CAMARGO	9 de abril de	Enabled	Primary	
9	PeopleSoft_UM_HR	Peoplesoft User HR	C.CAMARGO	22 de enero	Enabled	Primary	
10	PeopleSoft_UM_Finanzas	Peoplesoft User FN	426214	17 de mayo d	Enabled	Primary	
11	Egresados	EgresadoPUJ	430591	19 de mayo d	Provisioned	Primary	
12	Egresados	EgresadoPUJ	533512	28 de agosto	Provisioned	Other	

Filas Seleccionadas 1



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 envío automático de correo de autoregistro.
 - Nuevos perfiles de PS sin email.
 - Cargue de cuentas a BlackBoard



Gestión de Identidades - Retos

- Calidad de datos: correo alternativo, 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

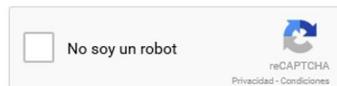
- Las preguntas y respuesta reto: SON UN RETO!!



Cambio de contraseña

A continuación puedes iniciar el cambio de contraseña para tu cuenta institucional mediante la plataforma TuID. A continuación Ingresar tu cuenta institucional.

Cuenta: * @javeriana.edu.co



Registrar

Pontificia Universidad Javeriana • Bogotá D.C. • Dirección de Tecnologías de Información •
Contáctenos: Servir-T | Tel. (57 1) 3208320 ext 5555



Cambio de contraseña

Para validar tu identidad te enviaremos un código de verificación. ¿A dónde deseas recibir este código?

- Correo alternativo: ngo*****@gmail.com
- Teléfono móvil: *****8478

Enviar **Cancelar**

Pontificia Universidad Javeriana • Bogotá D.C. • Dirección de Tecnologías de Información •
Contáctenos: Servir-T | Tel. (57 1) 3208320 ext 5555



Gestión de Identidades - Retos



Permisos para el Sistema de Información Universitario (PeopleSoft)

Inicialmente se puede solicitar permisos del módulo de compras de bienes y servicios (PO), Control de Compromisos y Presupuesto (KK) y Modulo de Recursos Humanos(RH))
[\[Ver más \]](#)

Categorías

- Módulo de Recursos Humanos
- Operaciones Internas y Control de compromisos
- Solicitud de compras de bienes y servicios

Módulo de Recursos Humanos

¿Dudas en la selección de estos permisos?
Solicite asesoría en la Dirección de Gestión Humana en la Ext. 2340.

Aprobador Selección
Permite participar en los procesos de selección y tomar decisión sobre los personas que ingresarán a la Universidad, hacen parte de los Workflow de Aprobación tanto para la creación de la Vacante como para la oferta económica al solicitante. También permite el acceso a los módulos de selección que permite crear vacantes, buscar solicitantes, consultar vacantes. [Agregar](#)

Consulta Unificación de Contratos
Permite consultar los contratos generados y unificados de Profe [Agregar](#)

Consultor Capacidad Endeudamiento
Permite consultar e imprimir la Capacidad de Endeudamiento [Agregar](#)

Consultor Datos Basicos
Este componente, le permite al usuario consultar los datos básicos de contacto y personales de los trabajadores de la Universidad (Nombres Completos, Identificación, Dirección Domicilio, Teléfono, Nivel S [Agregar](#)

Consultor Datos Puesto
Este componente, le permite al usuario consultar los datos laborales de los trabajadores de la Universidad (Fechas de Contratacion, Tipo de Contrato, Salario, Horas Semanales, etc.) [Agregar](#)

LISTADO DE ITEMS



Recuerde que debe contar con autorización de un jefe de unidad para solicitar cualquier permiso.

Total Permisos seleccionados: **0**

[Haz clic en un ítem para agregarlo a tu solicitud](#)

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



INICIO

MIS APPS

CERRAR SESIÓN

A continuación se encuentran tus aplicaciones. Ingresas haciendo clic en la imagen.



BI Estudiantes

Inteligencia de negocios para el componente de estudiantes.



BI Profesores

Inteligencia de negocios para el componente de profesores.



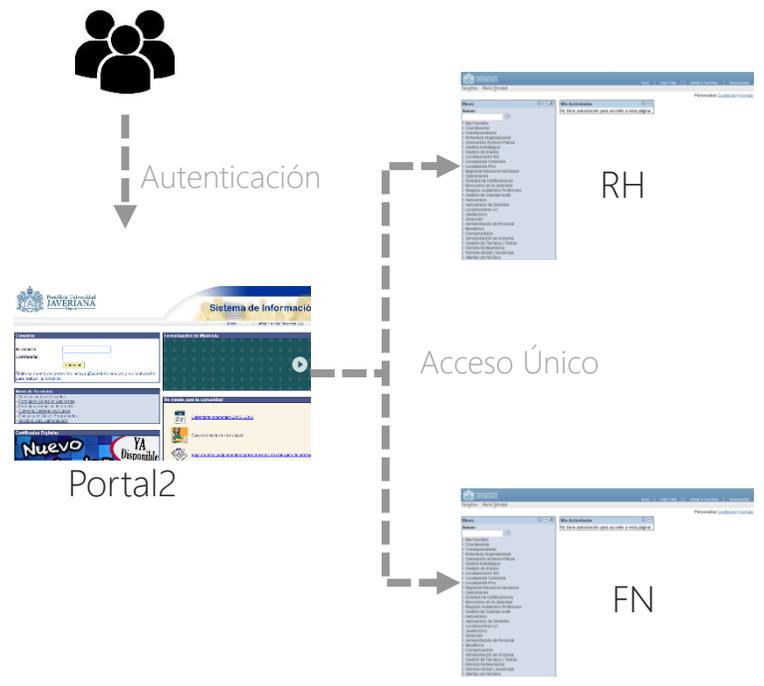
BI Administrativo

Inteligencia de negocios para el componente administrativo.



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,

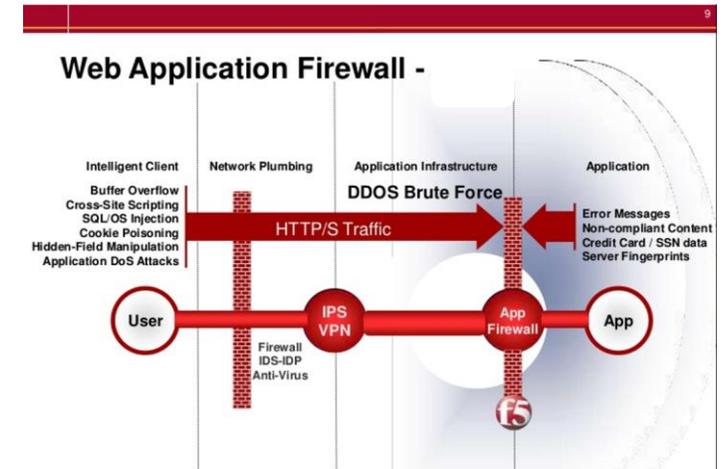


Seguridad en PS

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 componentes 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
Pontificia Universidad Javeriana
ngomez@javeriana.edu.co

