

## **Proyecto Portal de Recursos Humanos Experiencia en la implementación en la Universidad de Buenos Aires**

Rubén Darío Aybar<sup>a,1</sup>, Alex Fernando Flores<sup>a,2</sup>, Lilén Rocío Gordillo<sup>a,3</sup>, Ana Paula Vidal<sup>a,4</sup>

<sup>a</sup> Coordinación General de Tecnologías de la Información y las Comunicaciones, Universidad de Buenos Aires

Pte. Uriburu 860, Ciudad Autónoma de Buenos Aires, Argentina

<sup>1</sup>ruben.aybar@rec.uba.ar, <sup>2</sup>alex.flores@rec.uba.ar, <sup>3</sup>lgordillo@rec.uba.ar, <sup>4</sup>avidal@rec.uba.ar

**Resumen:** La presentación de este informe es dar cuenta de los aspectos técnicos, funcionales y del beneficio de la implementación de un portal online para el uso exclusivo de los agentes de la Universidad de Buenos Aires. Por lo general, los tiempos de consultas en las entidades educativas estatales argentinas suelen ser presenciales y burocráticos, lo que genera pérdida de tiempo valioso al interesado. En pos de agilizar estos procesos, a mediados del 2015, la Coordinación General de Tecnologías de la Información y las Comunicaciones patrocinado por la Dirección General de Recursos Humanos, desarrolló el Portal de Recursos Humanos de la Universidad de Buenos Aires. Este sistema cuenta con una instancia pública que permite la difusión ágil de noticias e información de interés general relacionadas a los Recursos Humanos y otra instancia privada que, a través de una identidad digital, habilita la consulta de información personal sensible a los docentes, no docentes y autoridades de la Universidad de Buenos Aires tal como los datos de contacto, del cargo, del título, la posibilidad de ingresar una licencia médica y controlar su estado, la descarga de los últimos doce detalles de haberes hasta el del mes inmediato anterior, la obtención de la credencial ART<sup>1</sup> y la consulta de marcajes horarios. Esta herramienta es un punto de encuentro, de participación y consulta con la intención de seguir creciendo y desarrollándose de acuerdo a la necesidad de la institución y por ende, su personal.

**Palabras Clave:** Infraestructura y desarrollo de software, Difusión de la información, Portal de Recursos Humanos, Autogestión, SSO.

### **1 Introducción**

En los últimos diez años, la era digital ha evolucionado la vida de las personas en más de un aspecto. La existencia de internet y el uso de los aparatos electrónicos han dado impulso a este cambio cultural. El ámbito de la educación no es ajeno a ello y de manera progresiva se comenzó a utilizar esta metodología. La Universidad Virtual es más que la integración del personal en internet, implica colaboración y participación activa de todos los actores, simboliza la modernización de la universidad y la transparencia de los procesos administrativos para con su capital humano, concede

---

<sup>1</sup> Las Aseguradoras de Riesgos del Trabajo (ART) son empresas privadas contratadas por los empleadores para asesorarlos en las medidas de prevención y para reparar los daños en casos de accidentes de trabajo o enfermedades profesionales.

accesibilidad a la consulta de la información útil de manera ágil, rápida y confiable. La Universidad Virtual es una propuesta que busca robustecer el uso de las nuevas Tecnologías de la Información y la Comunicación y fomentar la interacción entre los actores de la universidad. El proyecto se originó a partir del acercamiento del Director General de Recursos Humanos de Rectorado y Consejo Superior (DGRH) de la universidad a la Coordinación General de Tecnologías de la Información y las Comunicaciones (CGTIC) con un prototipo de una web en búsqueda de una solución integral para lograr un alcance masivo en la difusión de información e innovar y ampliar el sector. Los mismos apuntaban a optimizar los tiempos y la calidad de los procesos administrativos por medio de una herramienta de gestión autónoma, la difusión de normativa y reglamentación de la institución y con la posibilidad de aumentar la interacción con los docentes, no docentes y autoridad.

Luego de analizar con detalle el alcance del proyecto, desde CGTIC, se dio prioridad debido al salto cualitativo que implicaría integrar al personal a una Universidad virtual y por la factibilidad del proyecto, es decir, contar con los recursos necesarios para poder implementarlo y la excelente predisposición de la DGRH. Por esta razón el proyecto comenzó en el mes de Mayo del 2015. El objetivo del mismo es la búsqueda de retroalimentación entre los actores de la universidad y la expansión de la modalidad virtual en las diferentes áreas. El mismo contó con un grupo de equipo conformado por: la directora de proyecto, un grupo de analistas senior, de desarrolladores semi senior y senior y con administradores de sistemas operativos (Linux y Windows), de seguridad informática y de comunicaciones. Se reunieron periódicamente para definir aspectos funcionales y técnicos y así poder llevar a cabo el proyecto. El trabajo en equipo fue sinérgico ya que todos los sectores aportaron a la calidad y llegada a tiempo y forma a los entregables. Esta modalidad fue un acierto debido a que los usuarios pudieron seguir el crecimiento del proyecto y aportaron nuevas ideas que generaron un robustecimiento del portal a medida.

Es menester mencionar que hasta la salida a producción del Portal de Recursos Humanos, la mayor parte de los no docentes, docentes y autoridades no tenían manera de consultar de manera ágil los marcajes horarios, ni la información personal almacenados en el sistema de Recursos Humanos de la UBA. Los mismos debían dirigirse a la oficina física de la dependencia de Recursos Humanos. Asimismo, debían solicitar los últimos recibos de sueldos puesto que se los entregaban con retraso.

Por todo lo anterior, la solución propuesta constó de una instancia de libre acceso para la difusión de noticias e información de interés de Recursos Humanos y otra instancia exclusiva para la consulta personal. La primera se desarrolló con Microsoft Sharepoint 2013, que es una herramienta que permite la interacción del usuario final con una interface amigable y moldeable a su medida para una mejor colaboración con la comunidad. Mientras que la segunda fue desarrollada a medida por la Coordinación General de Tecnologías de la Información y las Comunicaciones (CGTIC) y permite la integración al agente proporcionando información personal y la opción de colaborar mediante correo electrónico en el caso de que la misma sea incorrecta.

## 2 La Solución

Tal como se mencionó en la introducción, debido a la necesidad del usuario de facilitar los procesos administrativos, difundir información de gran interés para la comunidad universitaria y facilitar la consulta de información de manera segura para cada empleado de la Universidad de Buenos Aires, se ideó una instancia de acceso general para la utilización y administración de la DGRH y otras direcciones; y otra privada para la visualización de información sensible de cada agente docente, no docente y autoridad. Por un lado, en la sección pública, se diseñó una solución autogestionable e intuitiva que le brinda el control al usuario final sobre la administración de contenido, es decir, la posibilidad de crear, editar, eliminar y aprobar páginas, fotos, vídeos, artículos, etc. Además se los capacitó y se les facilitó manuales de uso.

La página principal del dominio <https://rrhh.uba.ar/> se divide en un header, navegador, body y footer. En el primero se observa el logo de la universidad y el título del portal. El segundo contiene iconos que redirigen con páginas del portal: “Inicio” que es el home, “Contacto” que lleva a la página de contactos con marcadores de ubicación en el mapa usando Google Maps API y teléfonos de las dependencias y subdependencias de la universidad. El icono a su derecha es “Noticias”, que es el listado de las noticias que el usuario comparte, y por último “Sitios de Interés” donde se encuentran los enlaces a las diferentes unidades académicas, hospitales, sitios UBA y externos. Asimismo hay un vídeo explicativo de “¿Cómo gestionar el acceso?” (a autogestión) que es una aplicación web que permite a los agentes UBA visualizar la información personal que tiene el sistema de Recursos Humanos de la UBA, y la opción “Ingresar” para entrar a autogestión. La misma se puede desplegar en otras tres posibilidades tales como “Activar usuario”, “Recuperar contraseña” y “Edición de datos”. Estos se detallarán más adelante en la instancia privada.

En el cuerpo se puede ver un carousel slider cuyo objetivo es colocar contenido dinámico y actual, en este caso imágenes y descripción respecto a las noticias que el usuario ingresa. Debajo del mismo, hay boxes con otras secciones del portal con mayor visibilidad y son: “Preguntas Frecuentes” con preguntas y respuestas recurrentes; “Normativa” que contiene un listado de la normativa de la universidad; “Capacitación” que son cursos para empleados No docentes que se dictan en el año por parte de la Dirección de Capacitación y Desarrollo (DCAP), dependiente de la DGRH; “Guía de trámites” que incluye instrucciones para realizar de manera eficiente trámites comunes a los agentes; “Colonia de Vacaciones” que contiene información sobre este servicio para los hijos de los agentes de la UBA. En el footer o pie de página figura el lugar donde fue desarrollado el sitio.



Fig. 1. Página principal del Portal de Recursos Humanos.

Por otro lado, la sección privada es una solución de autoconsulta llamado autogestión (<https://autogestion.rrhh.uba.ar>) por los agentes UBA, que permite el acceso a información personal a través de una autenticación administrada por “Tú cuenta portal” gestionada en la aplicación PWM<sup>2</sup>. El mismo accede a la base de LDAP<sup>3</sup> donde previamente se migró la información requerida para autogestión (nombre, apellido, número de documento, fecha de nacimiento, correo electrónico, etc.) desde el sistema de Recursos Humanos. Esto permite agilizar el proceso de la gestión de sus datos de autenticación desde dentro y fuera de la UBA.

Previamente se comentó que el agente debe gestionar a través del PWM una cuenta, no obstante a modo de seguridad para resguardar la identidad y por manejar información sensible, éste debe ser habilitado en el sistema de Recursos Humanos. Para ello debe ser habilitado por un enrolador capacitado, en el sector de Recursos Humanos correspondiente a cada dependencia. El mismo debe verificar la identidad del solicitante para habilitar el uso online. Una vez habilitado y con una cuenta activa el usuario puede ingresar a autogestión. Para facilitar los pasos previos y su uso, el equipo diseñó y subió un video de carácter explicativo sobre la habilitación de la

<sup>2</sup> PWM, Open Source Password Self Service for LDAP directories, es una solución en php (código abierto) de alta configuración que permite la implementación de un servicio web para la gestión cómoda y rápida por parte de los usuarios finales de su cuenta de usuario (Recupero de Password, Cambio de E-Mail, Seteo de preguntas para el Recupero de Password).

<sup>3</sup> LDAP son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero/Simplificado de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

cuenta e ingresar a autogestión. Además se agregó un instructivo descargable y una sección en preguntas frecuentes.



Fig. 2. Página de autenticación a “Tu cuenta Portal”.

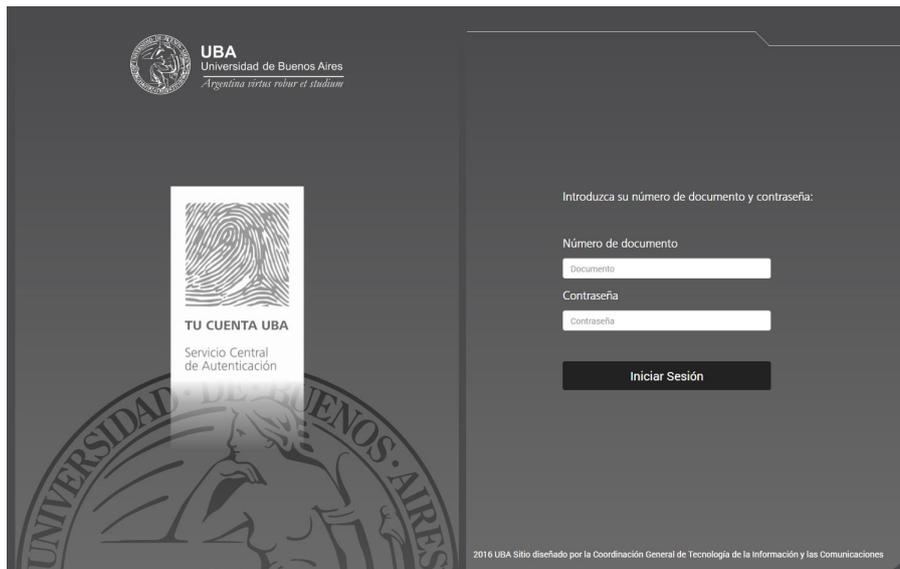


Fig. 3. Página de autenticación de autogestión.

El diseño es moderno adaptado a los esquemas actuales e intuitivo para un uso más sencillo del personal y la información proviene de la base de datos del Sistema de Recursos Humanos que actualiza diariamente las altas y/o actualizaciones del agente y de manera mensual la información relacionada a la liquidación de haberes a través

de un JOB<sup>4</sup> que se corre en horarios de poco uso para evitar el congestionamiento de la red.



Fig. 4. Página principal de Autogestión.

Dentro de la página se pueden ver diferentes iconos con información ordenada que le compete al no docente, docente y/o autoridad.

Formulario de Datos Personales:

Dirección: Calle (AMENABAR 661), Piso (3), Depto. (A), CP (1426).  
 Provincia (Capital Federal), Localidad (Capital Federal).  
 Correo (xxxxx@xxx.com.ar).  
 Teléfonos: Particular (47811043), Laboral, Celular.

Fig. 5. Datos Personales de Autogestión.

En la figura 5 se muestran los datos personales del agente autenticado tales como su domicilio, correo electrónico y teléfonos de contacto.

Descripción	Estado	F. Inicio	F. Fin	F. Baja	Tipo Documento	N Dec.	Emisor	Dependencia
Categoría 4 Admin Tempor	Activo (No Vencido)	23/12/2014	30/06/2017		Resolución Original	2279/14	Rector	Rectorado y Cons. Superior
Categoría 4 Admin Contra	Baja	01/01/2012	30/06/2015	23/12/2014	Resolución Original	3040/11	Rector	Rectorado y Cons. Superior
Categoría 7 Admin Perman	Licencia	23/12/2014			Resolución Original	2279/14	Rector	Rectorado y Cons. Superior

Fig. 6. Consulta de Cargos de Autogestión.

En la figura 6, se visualizan los cargos actuales e históricos que conforman la carrera universitaria del agente.

<sup>4</sup> Un Job es un conjunto de instrucciones SQL en paquetes de datos (DTS), que se ejecutan de forma automática cada cierto intervalo de tiempo.

Fecha Presentación	Entidad Educativa	Tipo Título	Título	Fecha Otorgamiento
27/12/2016	Universidad de Buenos Aires	1 - 25% - AUT // NOD	Licenciado en Sistemas de Información	07/12/2016
06/01/2011	Escuela Secundaria Privada	4 - 17,5% categoría 7 - NOD	Bachiller	16/12/2005

**Fig. 7.** Consulta de Cargos de Títulos.

En la figura 7, se pueden consultar los títulos informados al sistema de Recursos Humanos.

Tipo y Nro. Doc	Fecha Presentación	Parentesco	Apellido y Nombre	Sexo	Fecha Nacimiento	Edad	Discapacitado
DNI xxx	22/03/2012	Cónyuge	XXX	F	15/06/1988	28	No

**Fig. 8.** Consulta de Familiares.

En la figura 8, se ven los familiares declarados por el agente y su vínculo con el mismo.

Rectorado y Cons. Superior - Categoría 4 Admin Tempor

Buscar: (Ej: 01/03 ó Rec)

[Ingresar pedidos médicos](#)

Num. llamado	Tipo de licencia	Estado	Desc. llamado	Fecha de llamada	Fecha de inicio	Fecha de reincorporación
262131	Licencia de Corto Tratamiento	Resuelto	Licencia por Enfermedad del Titular	22/12/2016	22/12/2016	24/12/2016
248857	No Atendido o No Válido	Resuelto	Licencia por Enfermedad del Titular	26/08/2016		
224094	-	Aprobado	Licencia por Enfermedad del Titular	21/01/2016		
214196	Licencia de Corto Tratamiento	Resuelto	Licencia por Enfermedad del Titular	05/10/2015	05/10/2015	06/10/2015
200916	Licencia de Corto Tratamiento	Resuelto	Licencia por Enfermedad del Titular	18/06/2015	18/06/2015	20/06/2015

Resultados 1-5 de 17

Ingresado - Aprobado - Atendido - Resuelto

**Fig. 9.** Consulta de Licencias por Enfermedad.

En la figura 9, se encuentra el registro de las licencias por enfermedad y su estado actual y un buscador que encuentra cualquier coincidencia. No es de menor importancia mencionar que desde esta sección, los agentes, pueden generar un trámite de pedido médico<sup>5</sup>. Antes solo podían llamar a la oficina de asistencia en un horario específico para dejar asentado la inasistencia por enfermedad; hoy existe la posibilidad de tramitarla online o llamar. El Portal de Recursos Humanos interactúa en línea con el sistema de Licencias por lo cual no entorpece con el camino administrativo del segundo. Se le informó al usuario del sistema de Licencias la manera de distinguir los pedidos online: el usuario se lo registró como “autogestión”.

Buscar: (Ej: 01/03 ó Rec)

Fecha	Tipo Licencia	Tipo Cargo	Dependencia
07/12/2016	Trabajos Exteriores	Categoría 4 Admin Tempor	Rectorado y Cons. Superior
06/12/2016	Trabajos Exteriores	Categoría 4 Admin Tempor	Rectorado y Cons. Superior
05/12/2016	Compensatorio	Categoría 4 Admin Tempor	Rectorado y Cons. Superior
30/11/2016	Trabajos Exteriores	Categoría 4 Admin Tempor	Rectorado y Cons. Superior
29/11/2016	Día del No Docente	Categoría 4 Admin Tempor	Rectorado y Cons. Superior

Resultados 21-25 de 103

**Fig. 10.** Consulta de Licencias Laborales.

<sup>5</sup> Pedido medico: Trámite que se debe gestionar para avisar por enfermedad (del agente o familiar) a Recursos Humanos. Es necesario para que se admita en reconocimientos médicos. Éste es una oficina donde se va a justificar los días de ausencia por enfermedad.

En la figura 10, se muestran las licencias laborales ordenadas por la fecha más actual. También posee un buscador de las mismas características antes mencionadas.

Buscar: (Ej: 01/03 ó Rec)

Año	Tipo Licencia	Fecha Desde	Fecha Hasta
2016	Receso invernal	18/07/2016	22/07/2016
2015	Receso invernal	27/07/2015	31/07/2015
2015	Vacaciones	15/02/2016	05/03/2016

Resultados 1-3 de 3

**Fig. 11.** Consulta de Vacaciones.

En la figura 11, se ven las licencias anuales ordinarias ordenadas por año vencido y un buscador para agilizar la consulta.

Escalafon	Fecha Inicio Cargo	Fecha Antigüedad Relativa	Años	Meses	Días	Cant. años Liquidada
NOD	01/01/2012	01/01/2012	5	3	3	5

Resultados 1-1 de 1

**Fig. 12.** Consulta de Antigüedad

En la figura 12, se puede consultar la antigüedad por escalafón del agente. Todas las cabeceras de las consultas en grillas pueden ser ordenadas de manera ascendente o descendente.

Año:  Mes:

Abril

DO	LU	MA	MI	JU	VI	SA
						01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						



Datos del día 03 de Abril	
Entrada	10:18
Salida	18:27

Total de horas trabajadas 08:09

- ✓ Fichaje consistente
- ✗ Fichaje inconsistente
- Trabajo menos de 6.45 horas
- ▲ Ausencia de fichajes
- ▲ Dias feriados
- ▲ Justificación cargada

Total de horas trabajadas en el mes de Abril: 08:09

**Fig. 13.** Consulta de Marcaje Horario.

En la figura 13, se visualiza un calendario del mes vigente donde se podrá consultar los marcajes de entrada y salida por día y sus inconsistencias como por ejemplo ausencia de fichaje o un trabajo de menos de 6.45 horas. Además se pueden buscar años y fechas anteriores.

Detalles de haberes Periodo marzo 2017	↓
Detalles de haberes Periodo febrero 2017	↓
Detalles de haberes Periodo enero 2017	↓
Detalles de haberes Periodo diciembre 2016	↓
Detalles de haberes Periodo noviembre 2016	↓

[← Anterior](#)   [Siguiente →](#)

**Fig. 14.** Consulta de Detalle de Haberes.

En la consulta de Detalle de Haberes (figura 14) se ofrece la posibilidad de descargar en .pdf los últimos doce detalles de haberes. Por ultimo existe la opción de guardar en .pdf la credencial de la ART, facilitando la distribución de la misma.

### 3 Especificaciones Técnicas

#### 3.1 Aplicación

Para llevar a cabo la construcción del Portal de Recursos Humanos, la coordinación se inclinó por utilizar una plataforma de colaboración Microsoft Sharepoint 2013. Se la ha seleccionado debido que permite al usuario final una administración autónoma de contenidos a través de una interfaz amigable donde se pueden arrastrar y soltar archivos en bibliotecas de documentos, editarlas, tener vistas previas, compatibilidad con aplicaciones Microsoft Office, proporcionar entornos seguros para los administradores, perfiles personalizados, tener espacios de trabajo colaborativo y usar listas para ingresar registros.

La arquitectura de software de autogestión es MVC (modelo-vista-controlador) y es utilizada por prácticamente todos los framework. En este caso el mismo fue Microsoft .NET debido a la compatibilidad con las herramientas que utilizamos. Las aplicaciones que se comunican entre sí lo hacen por medio de la web api<sup>6</sup> y esto genera un ahorro de tiempo ya que éstas consumen los datos de la misma. Además evita que haya inconsistencia entre el funcionamiento de las distintas aplicaciones para una misma función. La comunicación de la web api con la aplicación web de autogestión se hace mediante Json por el protocolo HTTP. Como primera medida de seguridad se usa HTTPS para que los datos viajen de manera cifrada por internet y así nadie puede interceptar los paquetes y visualizar el contenido.

<sup>6</sup> Web API es un marco que facilita la creación de servicios HTTP disponibles para una amplia variedad de clientes, entre los que se incluyen exploradores y dispositivos móviles

**Tabla 1.** Especificaciones técnicas

Framework	Microsoft .NET 4.5
Patrón de arquitectura de software	MVC (model-view-controller)
Motor de vistas	Razor
Aplicación REST	ASP.NET Web api

### 3.2 Sistema de Autenticación y Autorización

Como método de autenticación y autorización se decidió incorporar el sistema Portal de Recursos Humanos al Proveedor de Identidad<sup>7</sup> (WSO2IS), el cual permite a los usuarios mediante procedimientos de SSO (Single Sign-On) acceder a los portales con los que ya cuenta la CGTIC.

Para comunicarse ambos sistemas en la actualidad se utiliza el protocolo WS-Federation (Passive) Configuration debido a su soporte nativo en aplicaciones ASP.NET, pero no es el protocolo que nos permite cumplir con los estándares de seguridad requeridos, ni se consiguieron los mejores resultados buscados, ya que solo es compatible con un solo browser (Chrome) y no funciona correctamente el logout entre otros problemas detectados.

Actualmente en los ambientes de test y desarrollo se está implementando una versión de prueba de la librería oficial del protocolo SAML<sup>8</sup> 2.0 de la empresa ComponentSpace<sup>9</sup> para ASP.NET (el trial dura 30 días), se decidió la utilización de este protocolo por cumplir con los estándares de seguridad requeridos para un sistema de autenticación y autorización de identidades y además por solucionar problemas de compatibilidad con los diferentes navegadores, con los tiempos de sesión, con el logout y también con la redirección luego de hacer logout, todos problemas que se encontraron con la utilización del protocolo WS-Federation (Passive) Configuration.

También cabe comentar que para el efectivo funcionamiento del protocolo SAML 2.0 en las aplicaciones desarrolladas en ASP.NET, se debe contar con la librería full, la cual también es comercializada por la empresa ComponentSpace y es necesario gestionar su compra en una etapa posterior del proyecto.

La CGTIC implementó su sistema de SSO basado en el software open source con licencia “Apache Software License Version 2.0” llamado WSO2 Identity Server que entre otros protocolos que soporta se encuentran, pero no se limitan, WS-Federation (Passive) Configuration y SAML 2.0 que eran requisitos necesarios para comenzar el proyecto, también se probó otra solución de SSO llamada CAS (Central Authentication Service) pero que no se ajustaba a las necesidades del proyecto. WSO2IS es una solución simple de instalar y configurar cumpliendo con los

<sup>7</sup> Un proveedor de identidad es un proveedor de confianza que le permite utilizar el inicio de sesión único para acceder a otros sitios Web.

<sup>8</sup> SAML (Security Assertions Markup Language) es un entorno basado en XML para servicios Web que permite el intercambio de información de autorización y autenticación entre diferentes sitios Web.

<sup>9</sup> <http://www.componentspace.com/Products.aspx>

requisitos previos, con una interface gráfica web de administración amigable para el administrador y en la que se pueden configurar todos los Service Provider, los Claims, los Usuarios y Roles locales y de los diferentes contenedores externos (en el caso del Portal de Recursos Humanos son directorios LDAP).

WSO2 Identity Server es un sistemas centralizado de autenticación y autorización (Single Sign-On), el cual le presenta una interfaz web al usuario que le permite ingresar sus credenciales digitales personales (Usuario y Password) para que luego el sistema pueda realizar la verificación de autenticación ante el directorio LDAP, y así acceder a los diferentes portales que son incorporados y pasan a delegar la gestión de las identidades de una forma segura y confiable. Asimismo sus cuentas son autorizadas con los niveles correspondientes de acceso para cada tipo de usuario en particular según los atributos que son devueltos de los directorios LDAP al Identity Provider.

### 3.3 Arquitectura del SSO (Single Sign-On)

La arquitectura del SSO (Single Sign-On) está compuesta por dos servidores virtuales con linux debian en modo clúster para el WSO2IS y un servidor virtual con linux debian para el PWM.

El flujo del sistema de SSO es iniciado por el SP (Service Provider), el usuario comienza en el sitio <https://rrhh.uba.ar> y, en lugar de iniciar sesión en el sitio <https://autogestion.rrhh.uba.ar> (SP), se inicia SSO con el IdP (Identity Provider), que en el caso del Portal de Recursos Humanos es <https://auth.rec.uba.ar>.

El diagrama de la figura 15 siguiente describe el flujo SSO iniciado por SP.

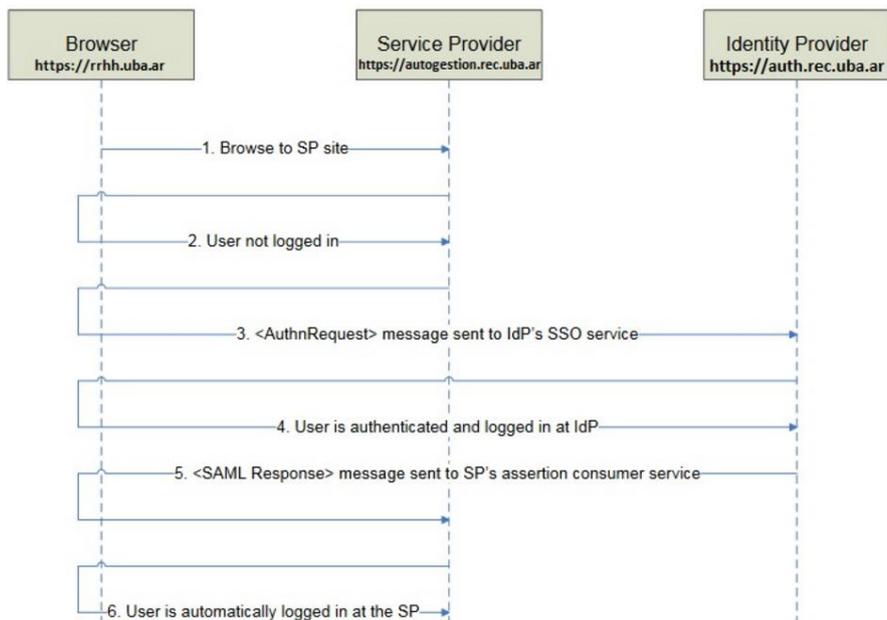


Fig. 15. SP inicializando SSO.

La explicación del diagrama es el siguiente:

1. El usuario navega el sitio <https://rrhh.uba.ar> desde su Browser.
2. Si intenta acceder a la página protegida <https://autogestion.rrhh.uba.ar> (SP) se le requiere autenticación.
3. El SP envía una solicitud de autenticación al punto final del servicio SSO del IdP.
4. Si aún no está autenticado en el IdP, debe presentar sus credenciales y loguearse en el portal <https://auth.rec.uba.ar> del IdP.
5. El IdP envía una respuesta SAML que contiene una aserción SAML al SP.
6. El SP utiliza la información contenida en la afirmación SAML, incluyendo el nombre del usuario y los atributos asociados, y realiza un inicio de sesión automático

A continuación se detallan los componentes más significativos del WSO2IS que son utilizados en la implementación del sistema de SSO de la CGTIC, destacando cuales son utilizados en el proyecto del Portal de Recursos Humanos, siendo el caso de:

- Soporte para Identity Provider y Service Provider (Service Provider)
- Soporte para diferentes Protocolos (WS-Federation (Passive) Configuration y SAML 2.0)
- Soporte para diferentes Repositorios de Usuarios (LDAP)
- Soporte para atributos de usuarios (Claims)

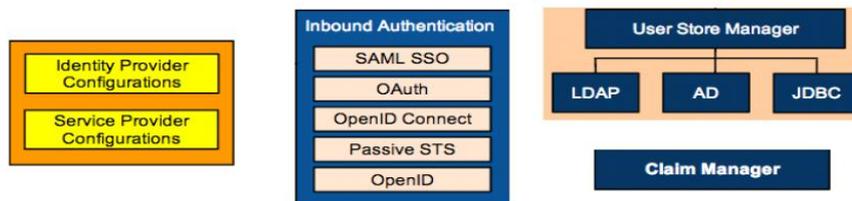


Fig. 16. Principales Componentes de WSO2IS.

### 3.4 Base de Datos:

Las bases de datos utilizadas en la implementación del proyecto fueron:

1. Microsoft SQL Server
2. MySQL
3. Ldap

Autogestión y Microsoft Sharepoint (Portal de Recursos Humanos) utiliza una plataforma de base de datos relacionales Microsoft SQL Server. Los datos de las

consultas de la instancia privada provienen del sistema de Recursos Humanos y éste fue diagramado en la herramienta de Microsoft por lo tanto por compatibilidad, las tablas nuevas de autogestión también. En cuanto a Microsoft Sharepoint, si bien es posible acceder a su base, no es recomendado por el prestador de servicio. El usuario final se maneja con listas, repositorios de imágenes, videos, páginas wiki<sup>10</sup> y artículos. WSO2IS utiliza MySQL como sistema de gestión de base de datos relacionales (RDBMS<sup>11</sup> del Inglés Relation Database Management Systems), la implementación del software es en modo clúster, es por ello que cada uno de los nodos tendrá una base de datos de registros locales y otra base de datos central para soporte de registro de configuración y gobernanza que será compartida por todos los nodos.

Database Name	Description
WSO2_USER_DB	JDBC user store and authorization manager
REGISTRY_DB	Shared database for config and governance registry mounts in the product's nodes
REGISTRY_LOCAL1	Local registry space in the manager node
REGISTRY_LOCAL2	Local registry space in the worker node

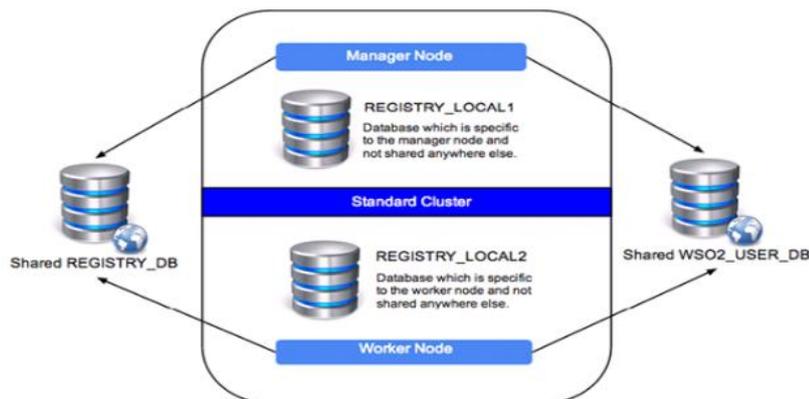


Fig. 17. Esquema de Bases de Datos de WSO2IS en Cluster.

LDAP<sup>12</sup> es un directorio que contiene información de forma jerárquica y categorizada, que puede incluir nombres, fechas y otros datos.

<sup>10</sup> Páginas Wiki son páginas web cuyo contenido puede ser editado por múltiples usuarios desde cualquier navegador.

<sup>11</sup> RDBMS es un programa que te permite crear, actualizar y administrar una base de datos relacional. La mayoría de los RDBMS comerciales utilizan el lenguaje de consultas estructuradas (SQL) para acceder a la base de datos, aunque SQL fue inventado después del desarrollo del modelo relacional y no es necesario para su uso.

<sup>12</sup> LDAP ("Lightweight Directory Access Protocol"), Protocolo de Acceso Ligero a Directorios es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio. Este se encuentra condensado en el estándar de Internet, el RFC 1777.

Las mayores ventajas de LDAP sobre las bases de datos relacionales son: rapidez en la lectura de registros, permitir replicar el servidor de forma muy sencilla y económica, dispone de un modelo de nombres globales que asegura que todas las entradas son únicas, usa un sistema jerárquico de almacenamiento de información, permite múltiples directorios independientes y funciona sobre TCP/IP y SSL.

En un primer momento se hizo una migración masiva de los datos almacenados en la base de datos relacional SQL Server del sistema de Recursos Humanos y en la actualidad se alimenta de las novedades de alta de cargo del mismo.

La finalidad del servidor LDAP es almacenar los usuarios y sus grupos de membresía para autenticar el Portal de Recursos Humanos. Se creó una estructura que parte de la base de nuestro directorio, la cual cuenta con una unidad organizativa denominada aplicaciones, para almacenar los grupos de usuarios y otra unidad organizativa llamada personas para almacenar a los usuarios. La organización de grupos de membresía es importante para la seguridad de la información para cada dependencia. Es decir, un usuario de la mesa de ayuda de una dependencia únicamente puede ver a los agentes de su misma dependencia.

### 3.5 Seguridad

El portal de Recursos Humanos cuenta con varias medidas de seguridad, la primera medida es la que protege por medio de un certificado digital SSL<sup>13</sup> (Secure Socket Layer) para cada uno de los sitios que componen el sistema completo: <https://rrhh.uba.ar>, <https://autogestion.rrhh.uba.ar> (autogestión), <https://auth.rec.uba.ar> y <https://usermanager.rec.uba.ar:8443> (PWM), y sirve para brindar seguridad a los visitantes, es decir una manera de informarles que el sitio es auténtico, real y confiable para ingresar datos personales.

Con lo explicado anteriormente se puede visualizar que la ventaja que trae para el Portal de Recursos Humanos el Certificado Digital SSL, desde el momento que el visitante puede entender que la transmisión de sus datos se está realizando de forma encriptada a través de internet que es un medio no seguro, y así confirmar que sus datos están libres de personas no deseadas.

---

<sup>13</sup> SSL es un protocolo de seguridad que permite que los datos viajen entre el servidor y el usuario y de modo inverso de una forma íntegra y segura, los datos no serán transmitidos en texto plano sino que serán cifrados o encriptados.

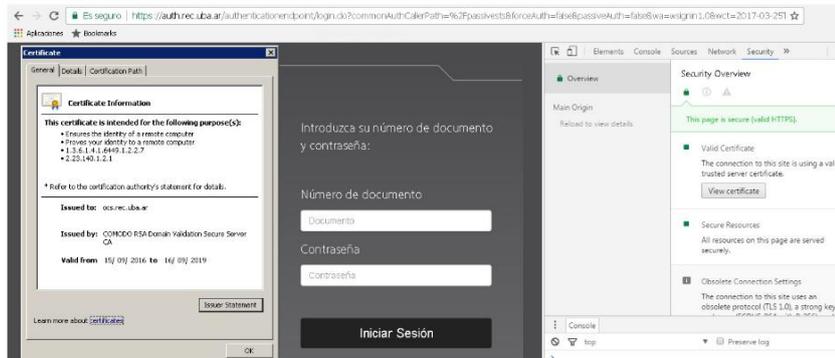


Fig. 18. Url de “Tu Cuenta UBA” con SSL y vista del Certificado.



Fig. 19. Url del “Portal de Recursos Humanos” con SSL.



Fig. 20. Url de “Autogestion” con SSL.



Fig. 21. Url de “Tu Cuenta Portal” con SSL.

Como segunda medida de seguridad “Tu Cuenta Portal” (PWM) utiliza el sistema de reCaptcha<sup>14</sup> ofrecido por Google, con ello se intenta proteger contra el Spam y las entradas no autorizadas al solicitar completar una simple prueba que demuestre que es un humano y no un ordenador quien intenta acceder a una cuenta protegida con contraseña.



Fig. 22. “Tu Cuenta Portal” Sistema de reCaptcha.

<sup>14</sup> Un CAPTCHA (test de Turing público y automático para distinguir a los ordenadores de los humanos, del inglés "Completely Automated Public Turing test to tell Computers and Humans Apart") es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta.

La seguridad del protocolo es muy importante ya que se encuentra presente al momento en el que el usuario se está autenticando y las especificaciones SAML recomiendan, y en algunos casos requieren una variedad de mecanismos de seguridad:

- SSL 3.0 o TLS 1.0 para la seguridad de nivel de transporte
- Firma XML y [Encriptación XML](#) para la seguridad a nivel de mensaje

Los requisitos son a menudo formulados en términos de autenticación (recíproca), integridad y confidencialidad, dejando la elección de mecanismo de seguridad para ejecutores e implementadores.

### 3.6 Infraestructura de Servidores

La infraestructura de Servidores es totalmente virtual con tecnología Vmware Esxi 5.5 y se destinaron los siguientes recursos:

Nombre	SO	Memoria	CPU		Storage
			vcpu	Procesador	
Sharepoint1.rec.uba.ar	Windows Server 2012 R2 Std	12	6	Intel® Xeon® CPU X5650 @ 2.67GHz	80GB
Sharepoint2.rec.uba.ar	Windows Server 2012 R2 Std	12	6	Intel® Xeon® CPU X5650 @ 2.67GHz	80GB
Sharepointdb1.rec.uba.ar	Windows Server 2012 R2 Std	14	12	Intel® Xeon® CPU X5650 @ 2.67GHz	155GB
Sharepointdb2.rec.uba.ar	Windows Server 2012 R2 Std	14	12	Intel® Xeon® CPU X5650 @ 2.67GHz	155GB
Sharepointtestigo.rec.uba.ar	Windows Server 2012 R2 Std	3	2	Intel® Xeon® CPU X5650 @ 2.67GHz	40GB
Autogestionw.rec.uba.ar	Windows Server 2008 R2 Ent	6	4	Intel® Xeon® CPU X5650 @ 2.67GHz	50GB
webwinext1.rec.uba.ar (web api)	Windows Web Server 2008 R2	6	4	Intel® Xeon® CPU E5530 @ 2.4GHz	60GB
prismadb.rec.uba.ar	Windows Server 2008 R2 Ent	18	8	Intel® Xeon® CPU E5-2680 @ 2.7GHz	650GB

**Fig. 23.** Detalle de recursos servidores.

La granja de SharePoint 2013 Server instalada con Sistema Operativo Windows Server 2012 R2 standar consta de dos front-end, un balanceador de carga, un servidor de aplicaciones y dos Servidores de datos SQL SERVER 2014 espejados. Se aplicó esta redundancia para asegurar la disponibilidad del servicio ante tareas de mantenimiento y contingencias. La infraestructura dedicada a SharePoint no es exclusiva del Portal de Recursos Humanos debido a que brinda servicios a diversos proyectos de Tecnologías de información y comunicaciones como sitios, sitios colaborativos, aplicaciones de inteligencia de negocios, servicio centralizado de proyectos, versionado de aplicaciones, etc.

Se configuraron tres rutas de acceso para este sitio con los siguientes proveedores de autenticación:

1. rrhh.rectorado.universidadba, destinada al acceso de administradores de Infraestructura, proveedor de autenticación Dominio de Active Directory.
2. rrhh.uba.ar, destinada para el acceso de empleados de la UBA. Acceso Anónimo.
3. rrhh.rec.uba.ar, destinada a administradores de contenidos, Proveedor de autenticación SSO.



desarrollo un requerimiento o un bug es a través de la herramienta Team Web Access 2010. La manera informal es por el correo electrónico interno por Microsoft Outlook y el chat interno Microsoft Lync. El uso de Microsoft SQL server 2012 y el Visual Studio 2013 para el desarrollo de autogestión por parte del área de desarrollo, el apache Directory Studio para la conexión con los directorios ldap (Desarrollo, Test y Producción), Sharepoint Designer 2013 para la parte pública del portal. Para el contacto entre las diferentes áreas de infraestructura, seguridad informática, infraestructura en linux, infraestructura en Windows, área funcional y área de desarrollo se utilizó el sistema de administración de Solicitudes técnicas desarrollado por la Coordinación General de Tecnologías de la Información y las Comunicaciones (CGTIC) llamado CIMA.

#### **4.2 Metodología de trabajo**

A lo largo del proyecto se ha incentivado la realización de reuniones periódicas con el objetivo de exponer los avances, dudas, inconvenientes, nuevos requerimientos, verificar las necesidades y facilitar la comunicación entre los miembros del equipo. La comunicación inter-áreas fue continua a través de los diferentes medios formales e informales mencionados en el punto anterior.

Se realizaron reuniones de colaboración y comunicación con los usuarios finales para relevar los requisitos, mostrar avances utilizando prototipos, definir prioridades del proyecto y estimar los tiempos de ejecución. Con la idea de mejorar la productividad y la calidad del Portal, el equipo analizó su modo de trabajo en los siguientes aspectos:

- Si el desarrollo de la solución funcionó bien.
- Si los entregables cumplieron las expectativas.
- ¿Cuál fue el feedback del usuario?
- Si la metodología adoptada fue eficiente.
- ¿Cuáles aspectos hay que mejorar?
- ¿Cuáles son los obstáculos que impidieron progresar?
- ¿Qué se ha aprendido en cada instancia del proyecto?

La modalidad utilizada permitió la sinergia del equipo; el aprendizaje sistemático fomentó la motivación de los miembros los cuales participaron en la mejora constante de la productividad y calidad del proyecto; la toma de decisiones en las distintas etapas fue consensuada y sostenible, esto ayudó a disminuir los obstáculos que se presentaron a lo largo del desarrollo; los resultados se pudieron visualizar en el corto plazo.

#### **4.3 Difusión del Proyecto**

La difusión del Portal se realizó por la DGRH con la ayuda de CGTIC. Una vez implementada la solución, se convocaron a los referentes de las Áreas de RRHH de las Unidades Académicas y Dependencias Hospitalarias a una reunión para la presentación formal de la herramienta. Se realizaron talleres de capacitación para saciar las inquietudes de algunos representantes y formar los enroladores designados quienes habilitan los agentes para que puedan ingresar a autogestión y a la mesa de ayuda. También se desarrolló un video de presentación con las indicaciones necesarias para autogestionar la activación del usuario, se subió en “Preguntas Frecuentes” un instructivo para el uso del Portal que se puede descargar en .pdf o leer online. Al día de hoy hubo poca difusión por parte de las dependencias, a excepción Rectorado y Consejo superior donde más se utiliza.

## **5 Perspectivas a Corto y Mediano Plazo**

En el corto plazo, nuestra perspectiva es que su implementación sea de uso masivo en toda la universidad, impulsar el crecimiento gracias al aporte de todos los no docentes, docentes y autoridades y fomentar el intercambio constante a través de las instancias virtuales como facebook, twitter y el correo electrónico de la DGRH. Se desea incorporar la edición de datos de contacto personal, de familiares y de títulos (para que luego sean aprobados por la Dirección de Recursos Humanos de su dependencia); la inclusión de la consulta al formulario 649<sup>15</sup> y de la correcta visualización en los distintos navegadores además de Google Chrome como por ejemplo Mozilla Firefox, internet explorer, Safari, etc.

En una instancia futura se planifica la incorporación de una ventanilla virtual que permitirá solicitar un trámite como por ejemplo un certificado de antigüedad a la Dirección de Recursos Humanos y poder hacer el seguimiento del mismo. Además, se proyecta desarrollar un aula virtual para la administración de contenido de los cursos de capacitaciones de docentes y no docentes que en el presente se gesta durante el año.

A un plazo más largo, se integrará la ventanilla virtual con el proyecto de firma digital automatizada para que el agente solicite trámites y pueda obtener los certificados firmados por la autoridad competente. Esto implicaría flexibilidad horaria, inmediatez y una reducción del uso de papel.

## **6 Conclusiones**

---

<sup>15</sup> Dicho Formulario es un resumen informativo del Año Fiscal anterior en donde se muestran las remuneraciones brutas, deducciones y retenciones sufridas en el Impuesto a las Ganancias. El Formulario sirve, en caso de corresponder, para confeccionar la Declaración Jurada del Impuesto a los Bienes Personales y del Impuesto a las Ganancias, según Resolución General AFIP N° 3839/2016. La AFIP es la Administración Federal de Ingresos Públicos. Se encarga principalmente de aplicar, cobrar e inspeccionar los tributos (ingresos públicos) de todo nuestro país y de controlar el tráfico internacional de mercaderías.

En Diciembre de 2016 se implementó el Portal de Recursos Humanos de la Universidad de Buenos Aires estableciendo un nuevo canal de comunicación en línea entre la Universidad y sus docentes, no docentes y autoridades en un contexto de innovación que posibilitan las tecnologías de la información y las comunicaciones en la Universidad del Siglo XXI.

El Portal de Recursos Humanos propone un punto de encuentro, de participación y colaboración con la intención de mejorar el servicio en un nuevo paradigma de gestión de los Recursos Humanos. El proyecto contempla diferentes fases de implementación, incorporando en cada una servicios que actualmente no están disponibles.

Si bien el Portal de Recursos Humanos está productivo entendemos que aún nos falta desarrollar más funcionalidades además de las previstas puesto que las necesidades del personal y de la institución son más abarcativas. Durante el transcurso del proyecto, el equipo se ha visto con diferentes obstáculos tanto funcionales como técnicos. En el aspecto técnico, el inconveniente dado fue el del cambio del protocolo de WS-Federation por SAML 2.0 que implicó modificar parte ya desarrolladas del sistema de Portal de Recursos Humanos por parte del equipo de desarrollo y la creación de nuevos Services Providers en el WSO2IS para SAML 2.0 por parte del equipo de Seguridad Informática y que puedan interactuar entre el Service Provider (SP) y el Identity Server (Idp). Esta decisión fue tomada debido a que SAML 2.0 cumple con los estándares de seguridad requeridos para un sistema de autenticación y autorización de identidades y además soluciona problemas de compatibilidad con los diferentes navegadores (permite el uso correcto del Portal en otros navegadores además del Google chrome) con los tiempos de sesión, con el logout y también con la redirección luego de hacer logout. La problemática funcional fue dada por la resistencia al cambio que manifestaron algunas dependencias al momento de ser difundido el proyecto. Las dudas recayeron en la funcionalidad y el pensamiento de que la herramienta era una manera de reemplazar las labores del personal. El temor fue disipado de manera inmediata al comunicar que el sistema sirve como un apoyo al trabajo y no como un reemplazante. En la actualidad, hay 2627 usuarios habilitados que pueden utilizar el servicio brindado por el portal; la cantidad de trámites de pedidos médicos es de 205.

## **Agradecimientos**

Los autores desean expresar su agradecimiento a la Lic. Sandra Barrios, Directora General de Sistemas Administrativos, Económicos y Legales de la UBA, por su aporte y participación en la puesta en marcha del Portal de Recursos Humanos y en el desarrollo de este trabajo.

## **Referencias**

1. WSO2 Identity Server, <http://wso2.com/identity-and-access-management>
2. SAML v2.0 for ASP.NET, <http://www.componentspace.com/SAMLv20.aspx>

3. CAS (Central Authentication Service), <https://apereo.github.io/cas/5.0.x/index.html>
4. Google reCaptcha, <https://www.google.com/recaptcha/intro/invisible.html>
5. Security Assertion Markup Language, [https://es.wikipedia.org/wiki/Security\\_Assertion\\_Markup\\_Language](https://es.wikipedia.org/wiki/Security_Assertion_Markup_Language)
6. Sharepoint 2013, <https://technet.microsoft.com/en-us/library/cc303422.aspx>
7. Model-View-Controller, <https://msdn.microsoft.com/en-us/library/ff649643.aspx>
8. AFIP, <http://www.afip.gob.ar/sitio/externos/>
9. Microsoft SharePoint es Marca Registradas de Microsoft.