

Implantación de adAS Integración con Office 365

Sergio Briongos Caballero

sbriongos@umh.es



Un poco de historia...

1997 – Inicio de sesión en las distintas aplicaciones contra LDAP/BBDD.

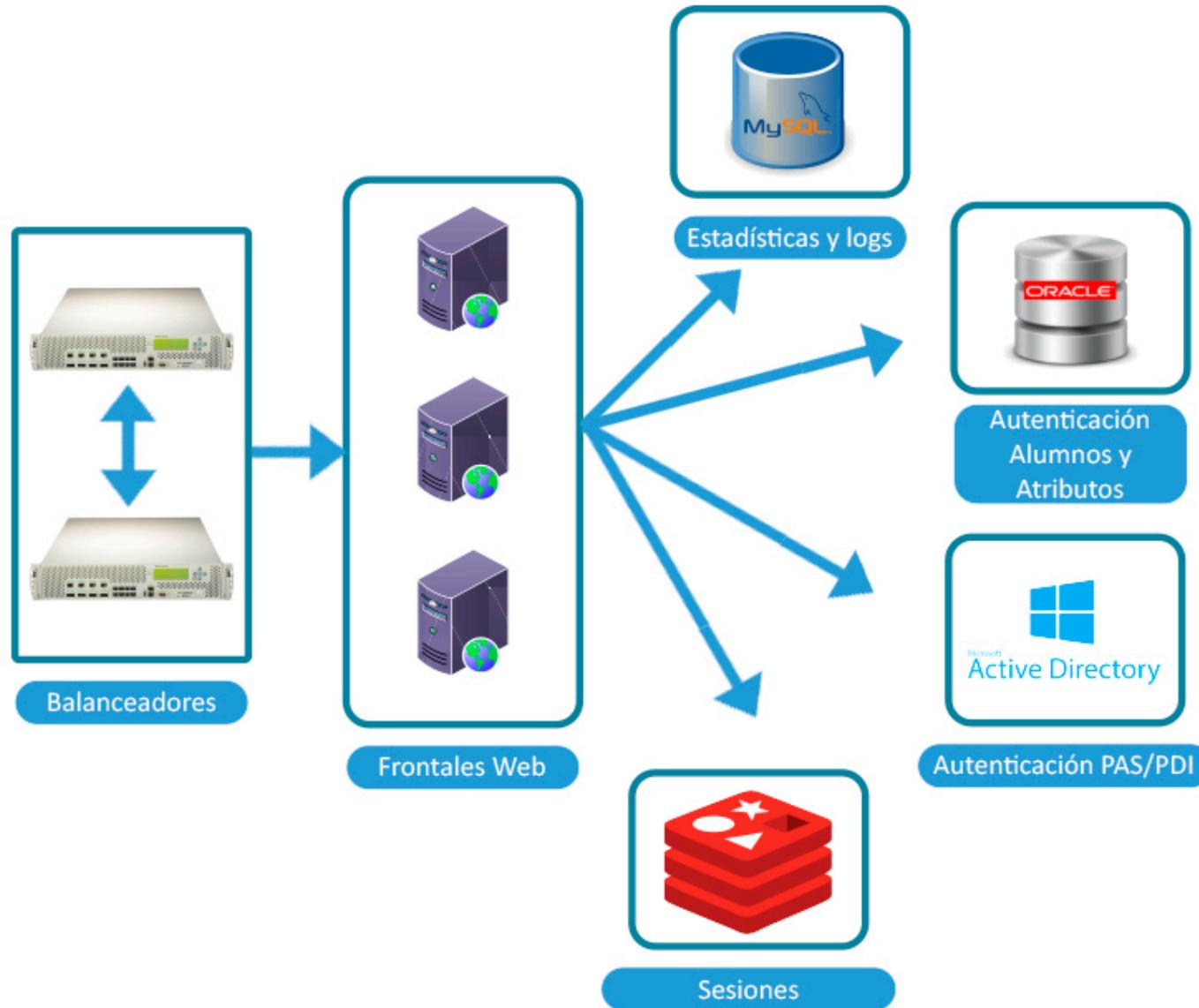
2007 – Se implanta Shibboleth como IDP y se empiezan a integrar aplicaciones bajo distintos SP.

2010 – Conocemos en las Jornadas Técnicas adAS.

11/2011 - Nos ponemos en contacto con Prise y comenzamos la integración.

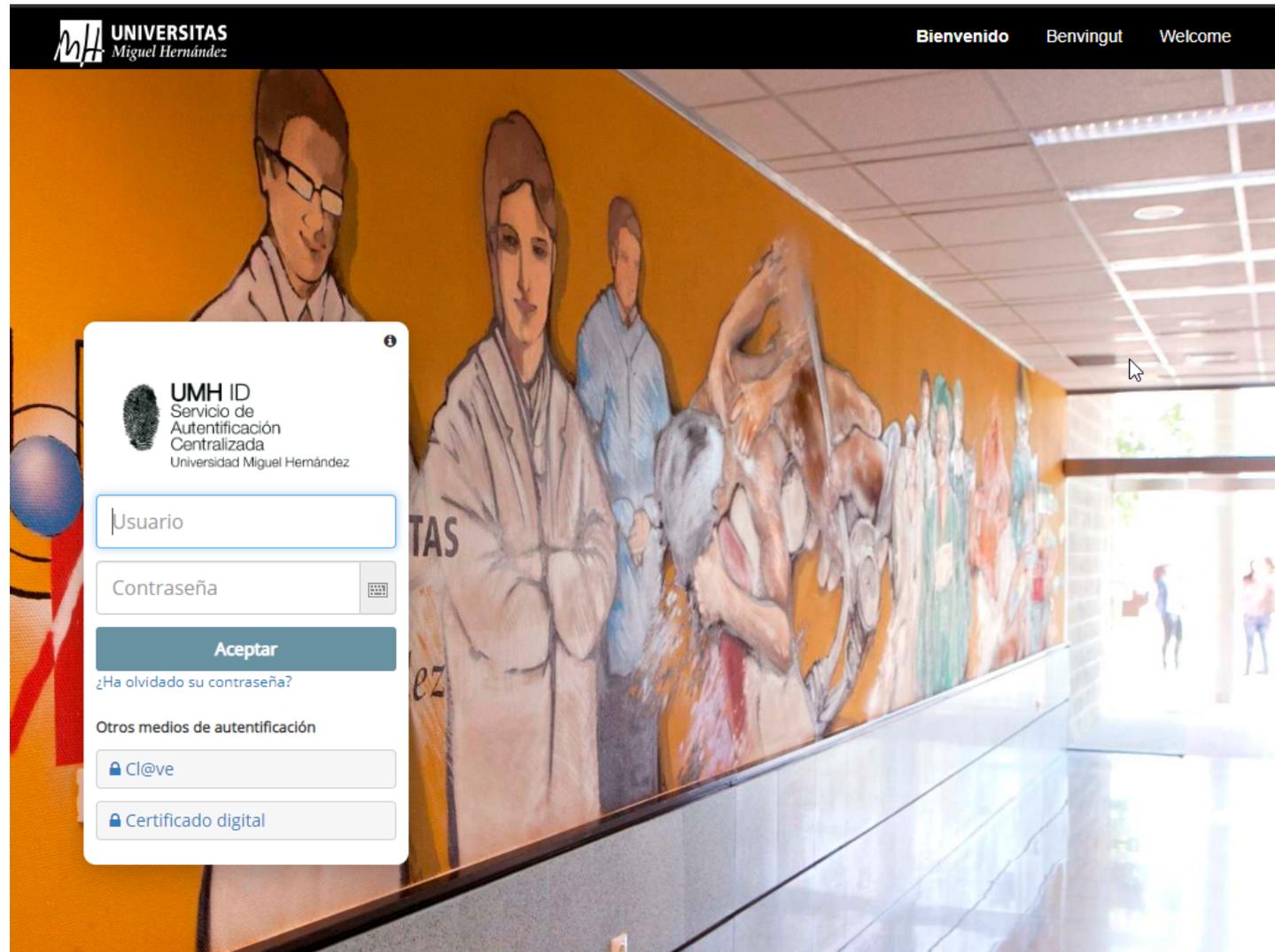
04/2012 – Terminamos la migración de nuestro IDP desde Shibboleth a adAS.

Arquitectura



Métodos autenticación:

- Usuario/contraseña
- Certificado electrónico o DNle
- Cl@ve (únicamente para la sede electrónica)



¿Cuándo comenzamos con Office365?

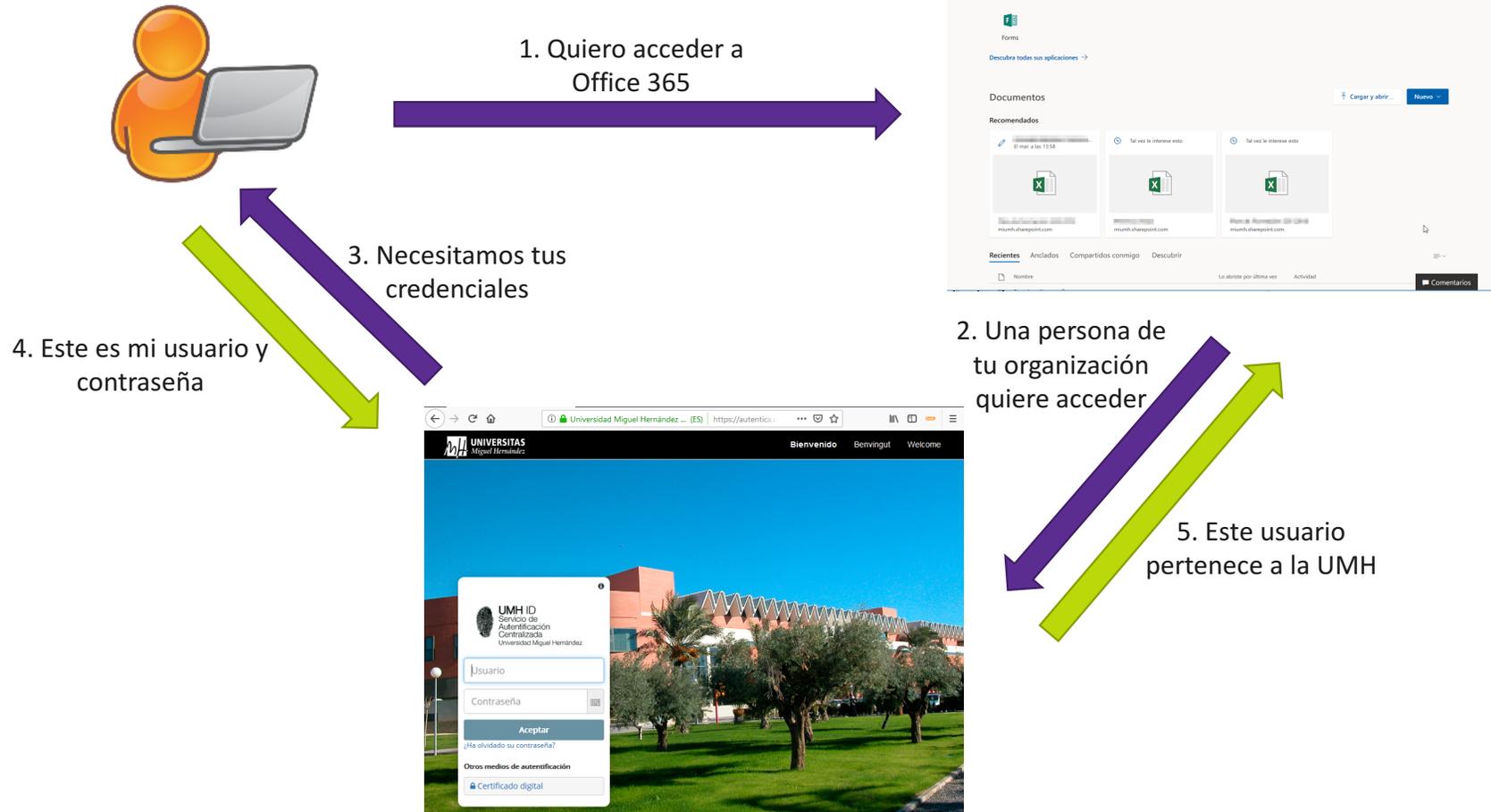
Octubre 2015 Comenzamos la integración Office365 en la UMH

Abril 2016 Primeras pruebas ECP de SAML

Julio 2016 Perfil ECP completamente operativo



Accediendo a través de https://portal.office.com

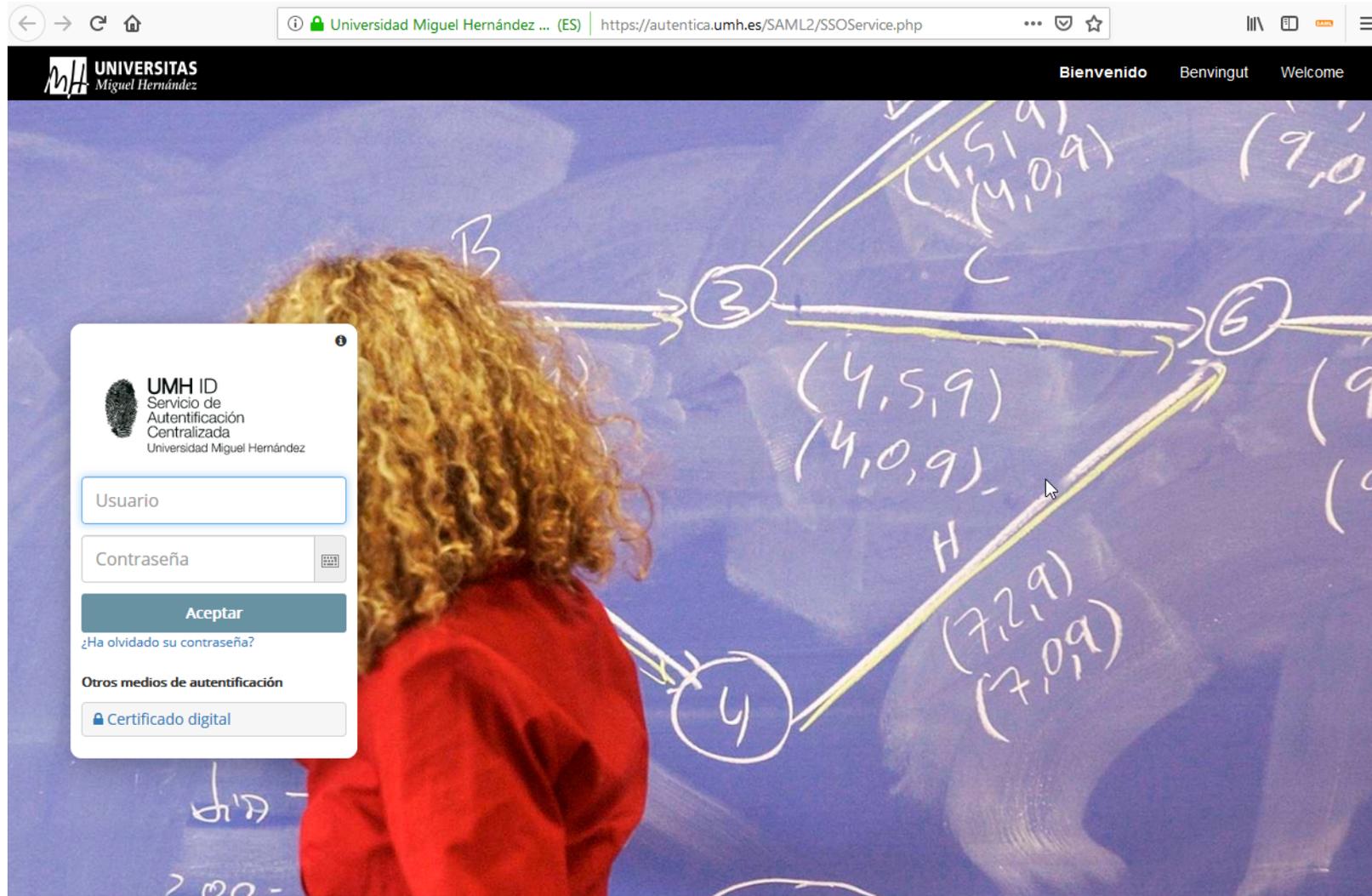


Accediendo a través de <https://portal.miumh.umh.es>



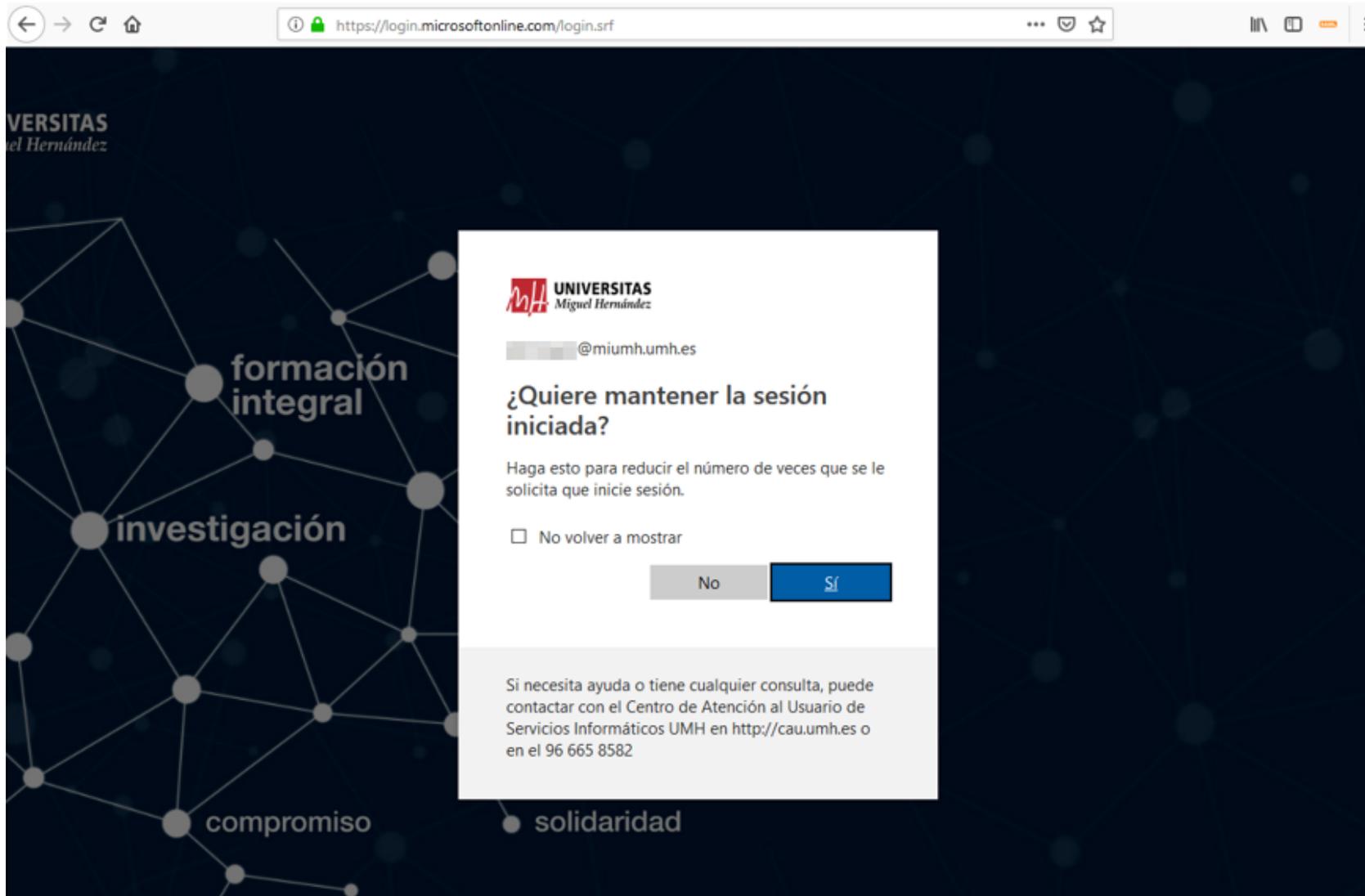
The screenshot shows a web browser at the URL portal.miumh.umh.es. The page features a header with navigation links for 'Acceso a MIUMH' and 'Soporte', and a search icon. Below the header is a large banner image of a desk with various office supplies, overlaid with the 'UNIVERSITAS Miguel Hernández' logo. A blue bar below the banner contains social media icons for Facebook, Twitter, and YouTube, with the text 'SEGUIR:'. The main content area is divided into three columns. The left column has a red 'Office 365 UMH' logo and text: 'Accede aquí a MIUMH' and 'Centro de aprendizaje de Office 365'. The middle column features a large image of a woman using a laptop in front of a building, with the 'Office 365' logo overlaid. Below this image is the text 'DESTACADAS 7 MARZO, 2017' and the article title '¿Qué es MiUMH?', followed by the introductory sentence 'Es el nuevo portal MIUMH (Office 365) mediante el cual estudiantes, profesores e'. The right column has a red 'MÁS' header and a section titled 'ENTRADAS RECIENTES' containing a list of recent articles: 'Acceso a un bloc de notas OneNote de un Grupo', 'Planner en Office 365', 'Limitación edición Excel Online y de escritorio', 'Instalacion de Word en Android', and 'Manual Class Notebook'.

Accediendo a través de <https://portal.miumh.umh.es>



The screenshot shows a web browser window with the URL <https://autentica.umh.es/SAML2/SSOService.php>. The page header includes the UMH logo and the text "UNIVERSITAS Miguel Hernández" on the left, and "Bienvenido Benvingut Welcome" on the right. The main content area features a chalkboard background with a graph. The graph has nodes labeled B, C, D, E, and H. Node B is at the top left, C is at the top center, D is at the top right, E is at the middle right, and H is at the bottom center. Arrows connect B to C, C to D, C to E, and D to H. Handwritten coordinates are visible: $(4,5,9)$ and $(4,0,9)$ near node C; $(7,2,9)$ and $(7,0,9)$ near node H; and $(9,0,1)$ near node D. A login form is overlaid on the left side of the chalkboard. The form is titled "UMH ID Servicio de Autenticación Centralizada Universidad Miguel Hernández" and includes fields for "Usuario" and "Contraseña", an "Aceptar" button, a link for "¿Ha olvidado su contraseña?", and a section for "Otros medios de autenticación" with a "Certificado digital" option.

Accediendo a través de <https://portal.miumh.umh.es>



UNIVERSITAS
Miguel Hernández

formación integral

investigación

compromiso

solidaridad

 UNIVERSITAS
Miguel Hernández

@miumh.umh.es

¿Quiere mantener la sesión iniciada?

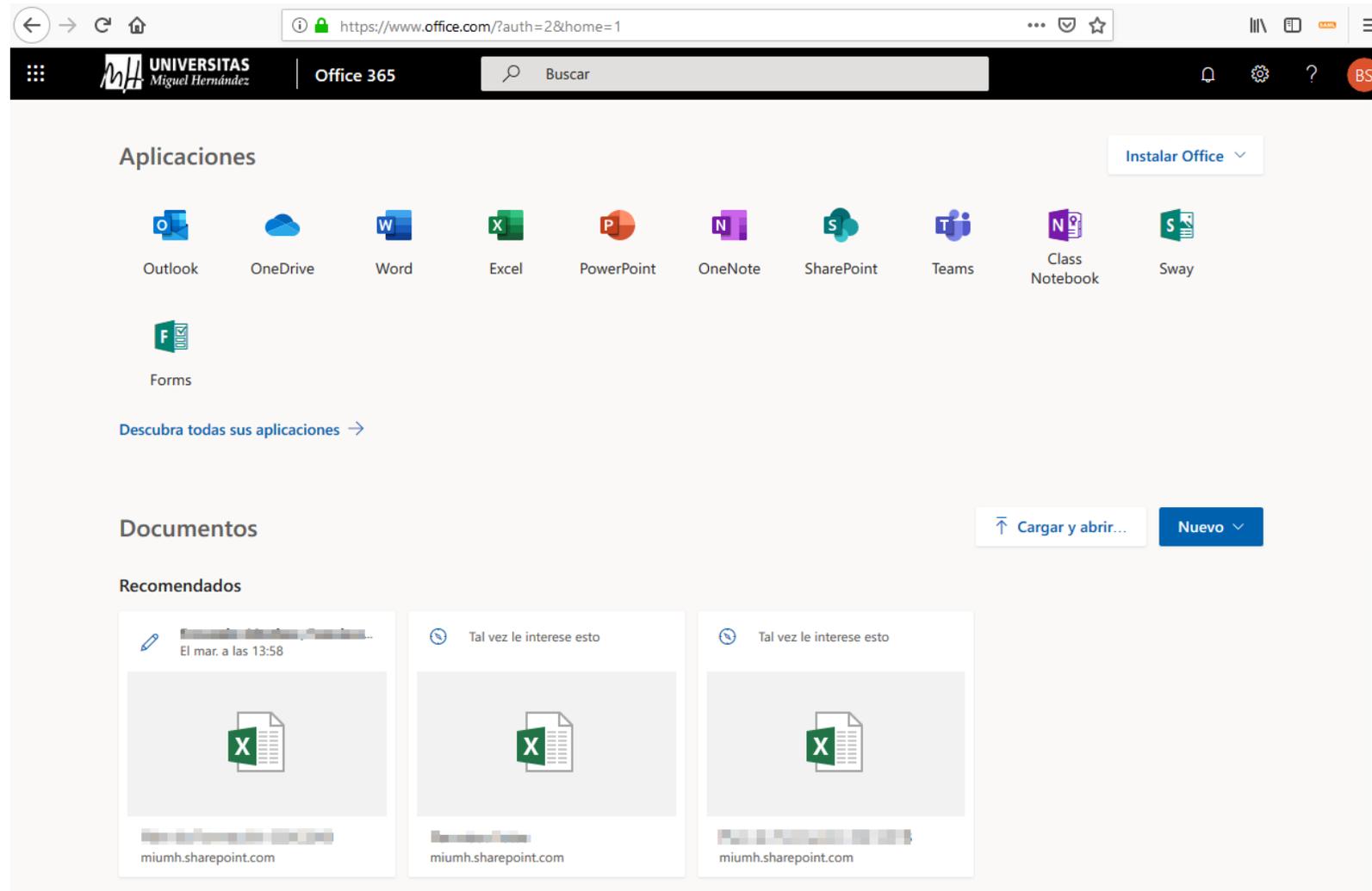
Haga esto para reducir el número de veces que se le solicita que inicie sesión.

No volver a mostrar

No Sí

Si necesita ayuda o tiene cualquier consulta, puede contactar con el Centro de Atención al Usuario de Servicios Informáticos UMH en <http://cau.umh.es> o en el 96 665 8582

Accediendo a través de <https://portal.miumh.umh.es>



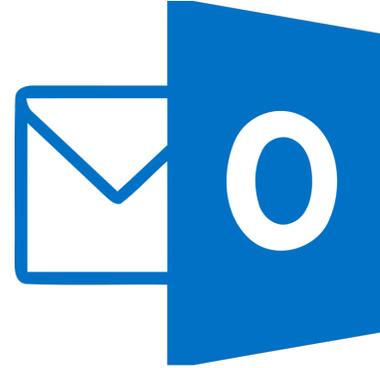
The screenshot shows the Microsoft Office 365 portal interface. At the top, the browser address bar displays <https://www.office.com/?auth=2&home=1>. The header includes the Universidad Miguel Hernández logo, the text "Office 365", a search bar with the placeholder "Buscar", and a user profile icon labeled "BS".

The main content area is divided into three sections:

- Aplicaciones:** A grid of application icons including Outlook, OneDrive, Word, Excel, PowerPoint, OneNote, SharePoint, Teams, Class Notebook, and Sway. A "Forms" icon is also present. A link "Descubra todas sus aplicaciones →" is located below the grid. A button "Instalar Office" is in the top right corner of this section.
- Documentos:** A section with a "Cargar y abrir..." button and a "Nuevo" button.
- Recomendados:** Three document cards, each featuring an Excel icon and the text "Tal vez le interese esto". The first card also includes the text "El mar. a las 13:58". All cards have a "miumh.sharepoint.com" link at the bottom.

Cientes de correo de escritorio

Microsoft Outlook: Exchange Web Services (EWS)



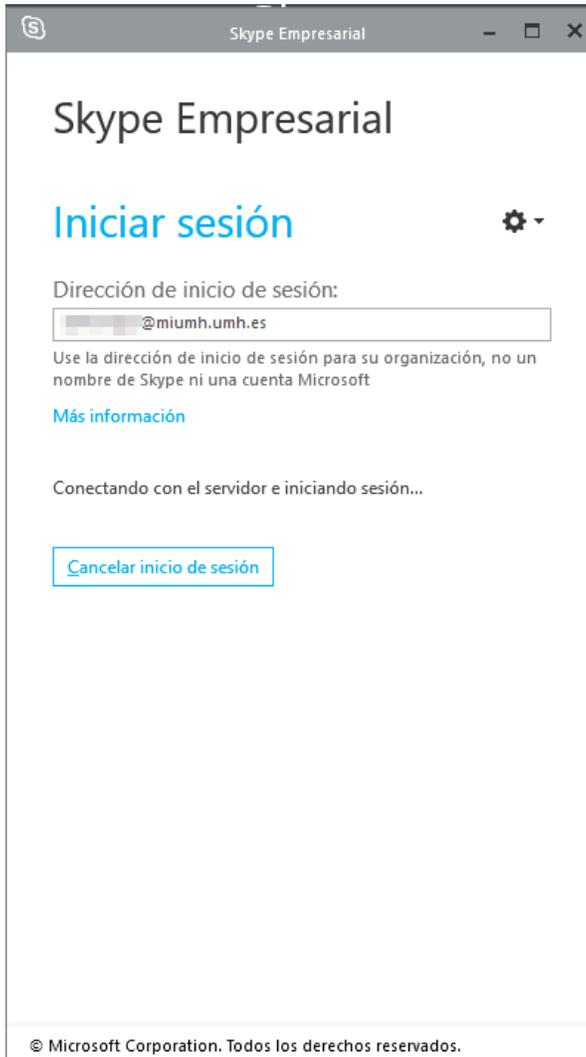
Mozilla Thunderbird: IMAP



Evolution: Exchange Web Services (EWS)



Skype empresarial



Skype Empresarial

Iniciar sesión

Dirección de inicio de sesión:

Use la dirección de inicio de sesión para su organización, no un nombre de Skype ni una cuenta Microsoft

[Más información](#)

Conectando con el servidor e iniciando sesión...

[Cancelar inicio de sesión](#)

© Microsoft Corporation. Todos los derechos reservados.



UNIVERSITAS Miguel Hernández

UMH ID

Servicio de Autenticación Centralizada
Universidad Miguel Hernández

Aceptar

[¿Ha olvidado su contraseña?](#)

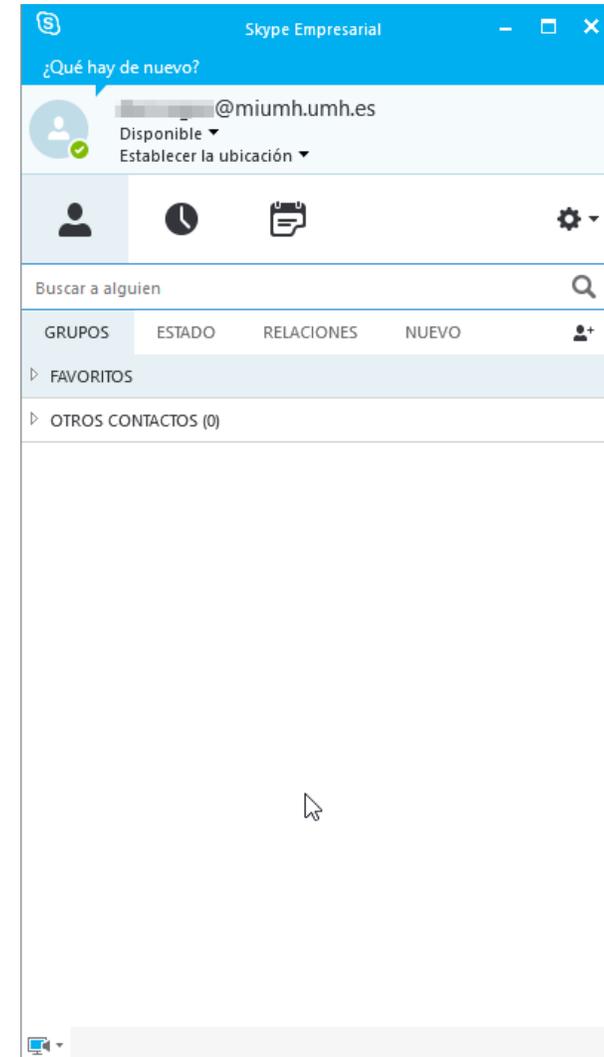
Otros medios de autenticación

Certificado digital

Bienvenido/a al **Servicio de Autenticación Centralizada de la UMH.**

El Servicio de Autenticación Centralizada de la UMH ofrece un mecanismo de identificación única, gracias al cual, podrá conectarse a todas las aplicaciones integradas con este servicio.

Su identidad, así como los privilegios que lleva asociados, serán recordados mientras no cierre la ventana del navegador o cierre la sesión.



Skype Empresarial

¿Qué hay de nuevo?

@miumh.umh.es
Disponibile
Establecer la ubicación

Buscar a alguien

GRUPOS ESTADO RELACIONES NUEVO

FAVORITOS

OTROS CONTACTOS (0)

Configuración en adas

Agregar metadatos de Microsoft.

Crear los atributos:

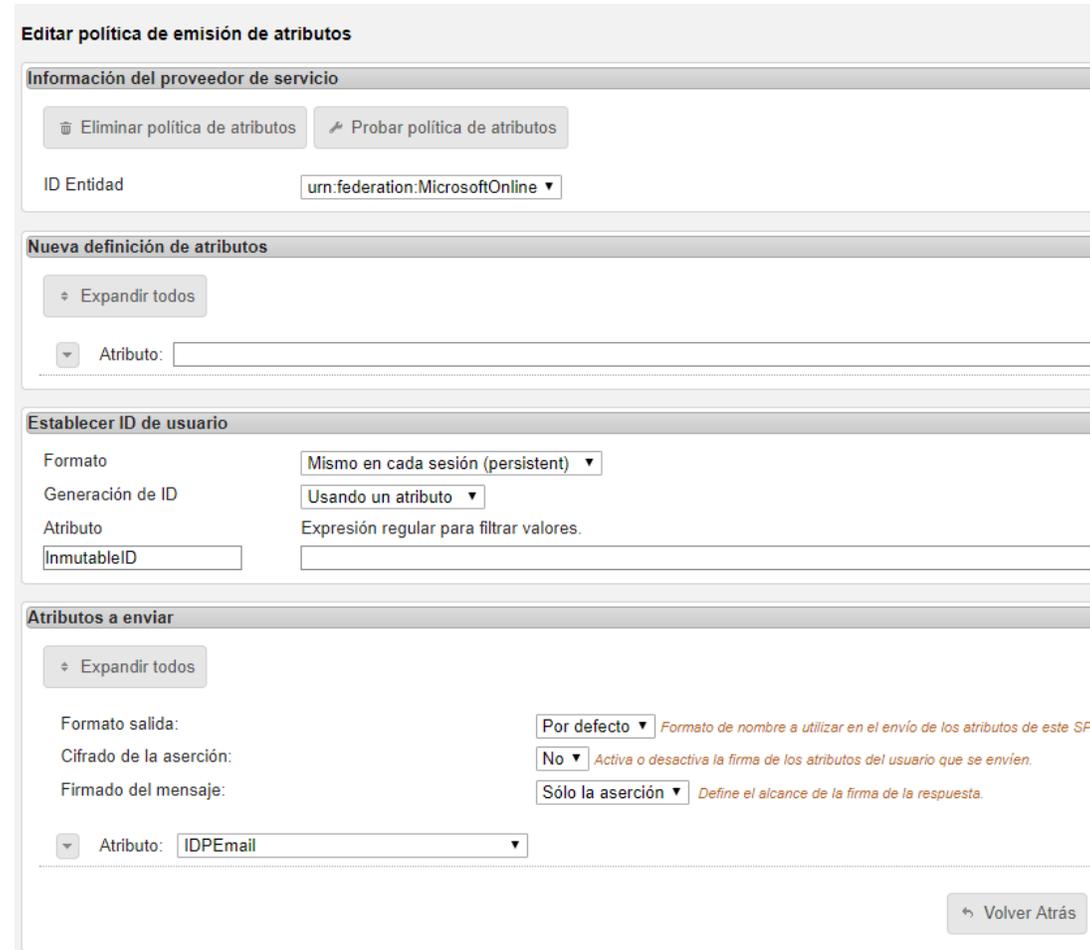
- ImmutableID
- IDPEmail

Establecer ID de usuario:

Formato persistent usando el ImmutableID

Importante:

- Firmar únicamente la aserción
- No cifrar la aserción
- Habilitar Perfil ECP en el protocolo SAML



The screenshot shows the configuration page for editing an attribute emission policy. It is divided into several sections:

- Editar política de emisión de atributos**: The main title of the page.
- Información del proveedor de servicio**: Contains buttons for 'Eliminar política de atributos' and 'Probar política de atributos', and a dropdown for 'ID Entidad' set to 'urn:federation:MicrosoftOnline'.
- Nueva definición de atributos**: Includes an 'Expandir todos' button and a dropdown for 'Atributo'.
- Establecer ID de usuario**: Contains dropdowns for 'Formato' (set to 'Mismo en cada sesión (persistent)'), 'Generación de ID' (set to 'Usando un atributo'), and 'Atributo' (set to 'ImmutableID'). It also has a text field for 'Expresión regular para filtrar valores'.
- Atributos a enviar**: Includes an 'Expandir todos' button, dropdowns for 'Formato salida' (set to 'Por defecto'), 'Cifrado de la aserción' (set to 'No'), and 'Firmado del mensaje' (set to 'Sólo la aserción'). It also has a dropdown for 'Atributo' set to 'IDPEmail'.

A 'Volver Atrás' button is located at the bottom right of the configuration area.

Aserción de ejemplo Office 365

```
<saml:Subject>
  <saml:NameID SPNameQualifier="urn:federation:MicrosoftOnline"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
    >18d9346[redacted]aa22f8[redacted]38d88</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2019-03-25T20:57:13Z"
      Recipient="https://login.microsoftonline.com/login.srf"
      InResponseTo="_51fa2f0c-1970-4d64-90fc-fecb06559d46"
      />
  </saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2019-03-25T19:57:11Z"
  NotOnOrAfter="2019-03-25T20:57:13Z"
  >
  <saml:AudienceRestriction>
    <saml:Audience>urn:federation:MicrosoftOnline</saml:Audience>
  </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2019-03-25T19:57:06Z"
  SessionIndex="_2d7b7f30-4f38-11e9-80fb-616263646566"
  >
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes>Password</saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    Name="IDPEmail"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
    >
    <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xsi:type="xs:string"
      >[redacted]@mihumh.umh.es</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Probando ECP

- Podemos probarlo con: <https://github.com/unikent-ms1/simple-soap-ecp-test>

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <ecp:Response xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp" AssertionConsumerServiceURL="https://login.microsoftonline.com/login.srf" soap:actor="http://schemas.xmlsoap.org/soap/actor/next" soap:mustUnderstand="1"/>
  </soap:Header>
  <soap:Body xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_89f71dc0-70a6-11e9-8097-6162636">
      <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://autentica.umh.es/SAML2/</saml:Issuer>
      <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </samlp:Status>
      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_89f71780-70a6-11e9-8064-616263646566" Version="2.0" IssueInstant="2019-05-07T09:00:19Z">
        <saml:Issuer>https://autentica.umh.es/SAML2/</saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
            <ds:Reference URI="#_89f71780-70a6-11e9-8064-616263646566">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>7.....=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>.....
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>.....
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
      <saml:Subject>
        <saml:NameID SPNameQualifier="urn:federation:MicrosoftOnline" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">18d93i.....de98d88</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
          <saml:SubjectConfirmationData NotOnOrAfter="2019-05-07T10:00:21Z" Recipient="https://login.microsoftonline.com/login.srf" InResponseTo=""/>
        </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2019-05-07T09:00:19Z" NotOnOrAfter="2019-05-07T10:00:21Z">
        <saml:AudienceRestriction>
          <saml:Audience>urn:federation:MicrosoftOnline</saml:Audience>
        </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2019-05-07T09:00:14Z" SessionIndex="_89f71780-70a6-11e9-8064-616263646566">
        <saml:AuthnContext>
          <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
        </saml:AuthnContext>
      </saml:AuthnStatement>
      <saml:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <saml:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Name="IDPEmail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
          <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">sbriogon@miumh.umh.es</saml:AttributeValue>
        </saml:Attribute>
      </saml:AttributeStatement>
    </saml:Assertion>
  </samlp:Response>
</soap:Body>
</soap:Envelope>
```

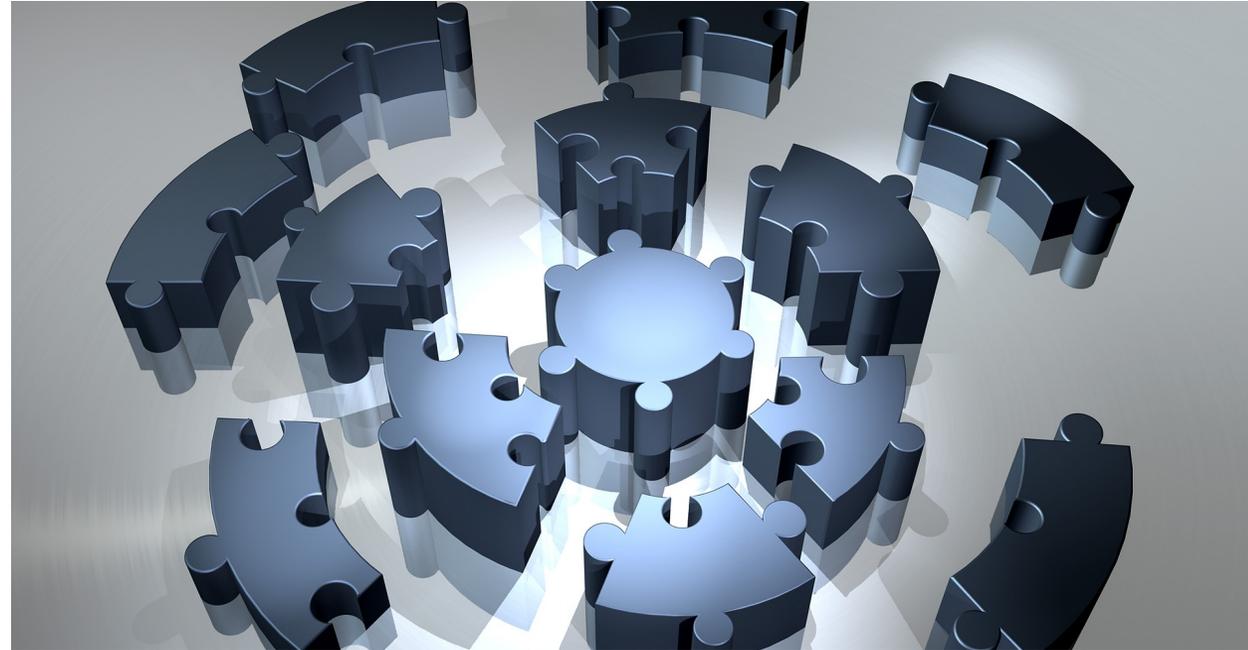
Scripts powershell para:

- Creación buzones
- Asignación licencias
- Cambios de login



Problemas encontrados y solucionados

- Cambios login: Pasar al usuario al dominio onmicrosoft, poner el ImmutableID a null, asignar el nuevo ImmutableID y volver a pasar al dominio federado.
- Cambios en el certificado del IDP: Poner el dominio en modo Managed, cambiar certificado y volver a poner en modo Federated.



Más información y dudas...

Gracias.

Sergio Briongos Caballero
sbriongos@umh.es

