Implantación de adAS
Integración con Office 365

Sergio Briongos Caballero
sbriongos@umh.es

UNIVERSITAS
Miguel Hernández

UNIVERSITAS
Miguel Hernández

Un poco de historia…

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

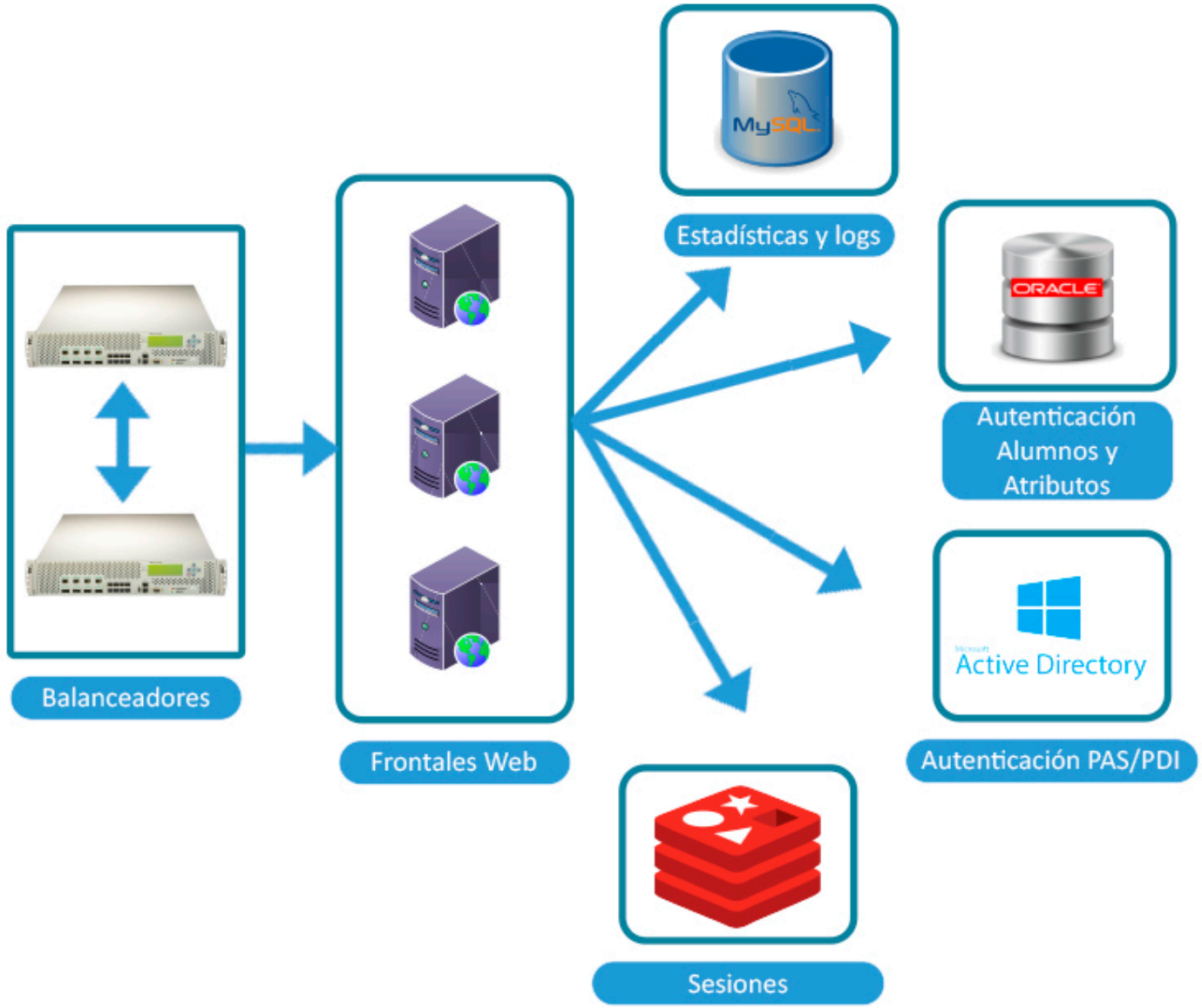
2007 – Se implanta Shibboleth como IDP y se empiezan a integrar aplicaciones bajo distintos SP.

2010 – Conocemos en las Jornada 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.

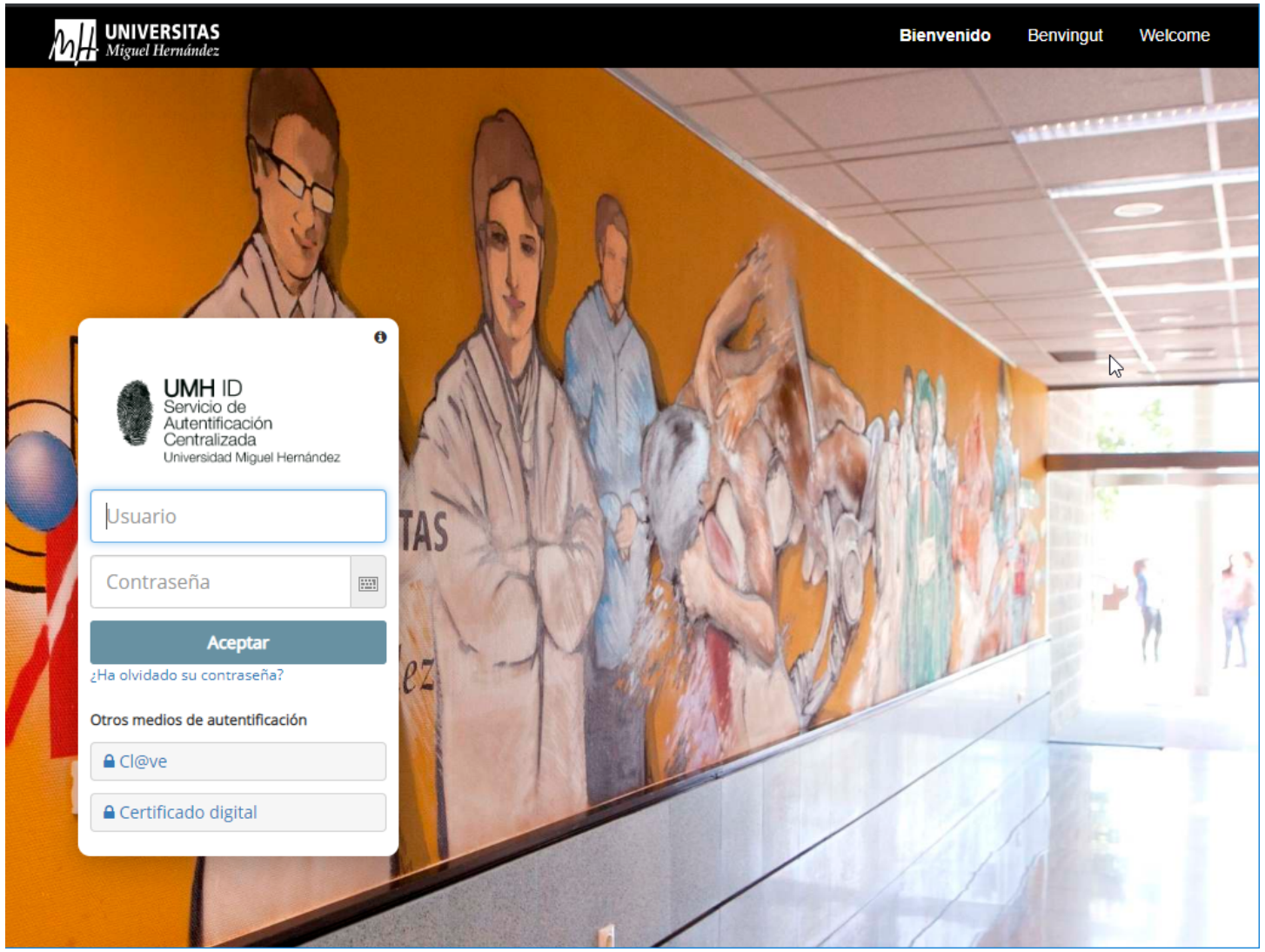
Arquitectura



Arquitectura

Métodos autenticación:

- Usuario/contraseña
- Certificado electrónico o DNIe
- 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

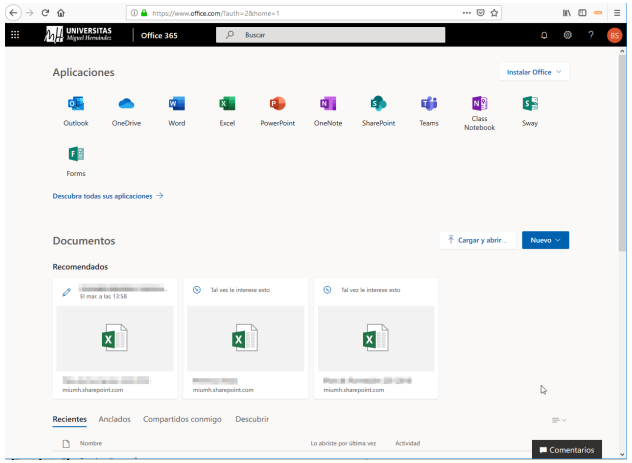
Julio 2016 Perfil ECP completamente operativo

UNIVERSITAS Miguel Hernández

UNIVERSITAS Miguel Hernández

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

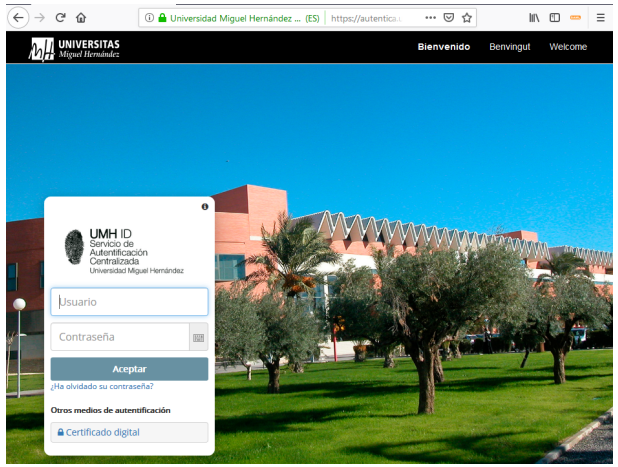
1. Quiero acceder a Office 365



2. Una persona de tu organización quiere acceder

3. Necesitamos tus credenciales

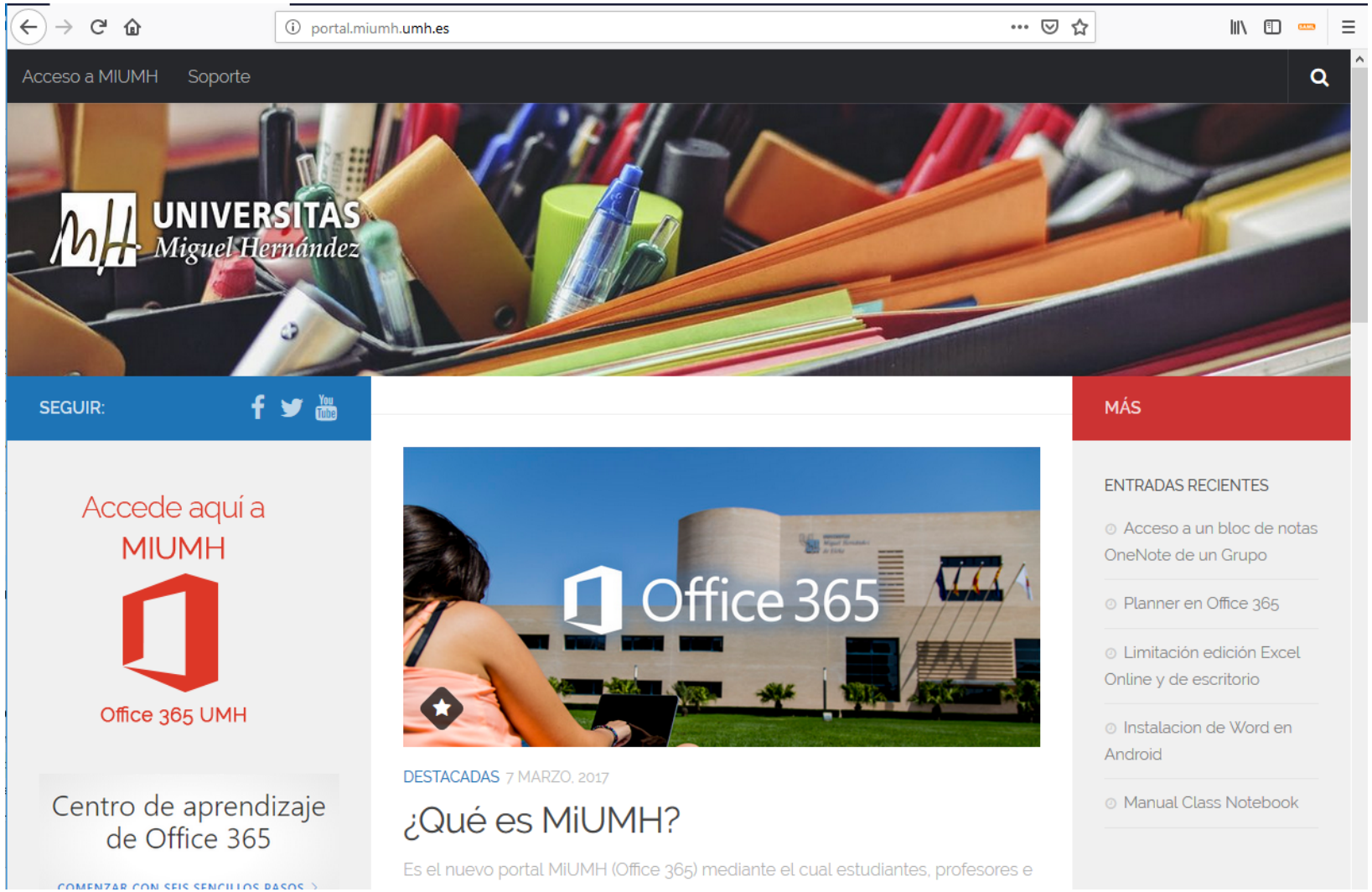
4. Este es mi usuario y contraseña



5. Este usuario pertenece a la UMH

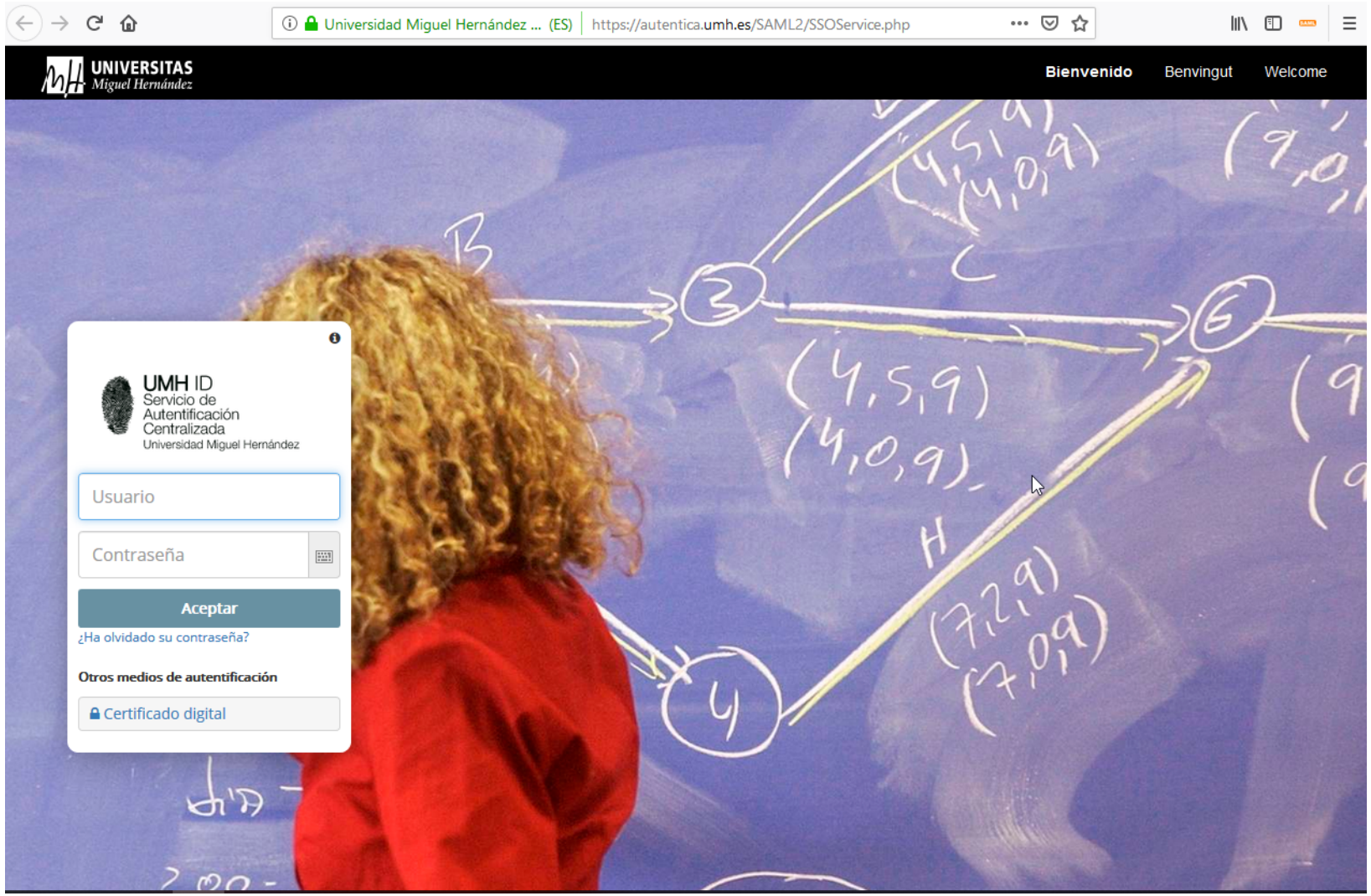
UNIVERSITAS Miguel Hernández

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

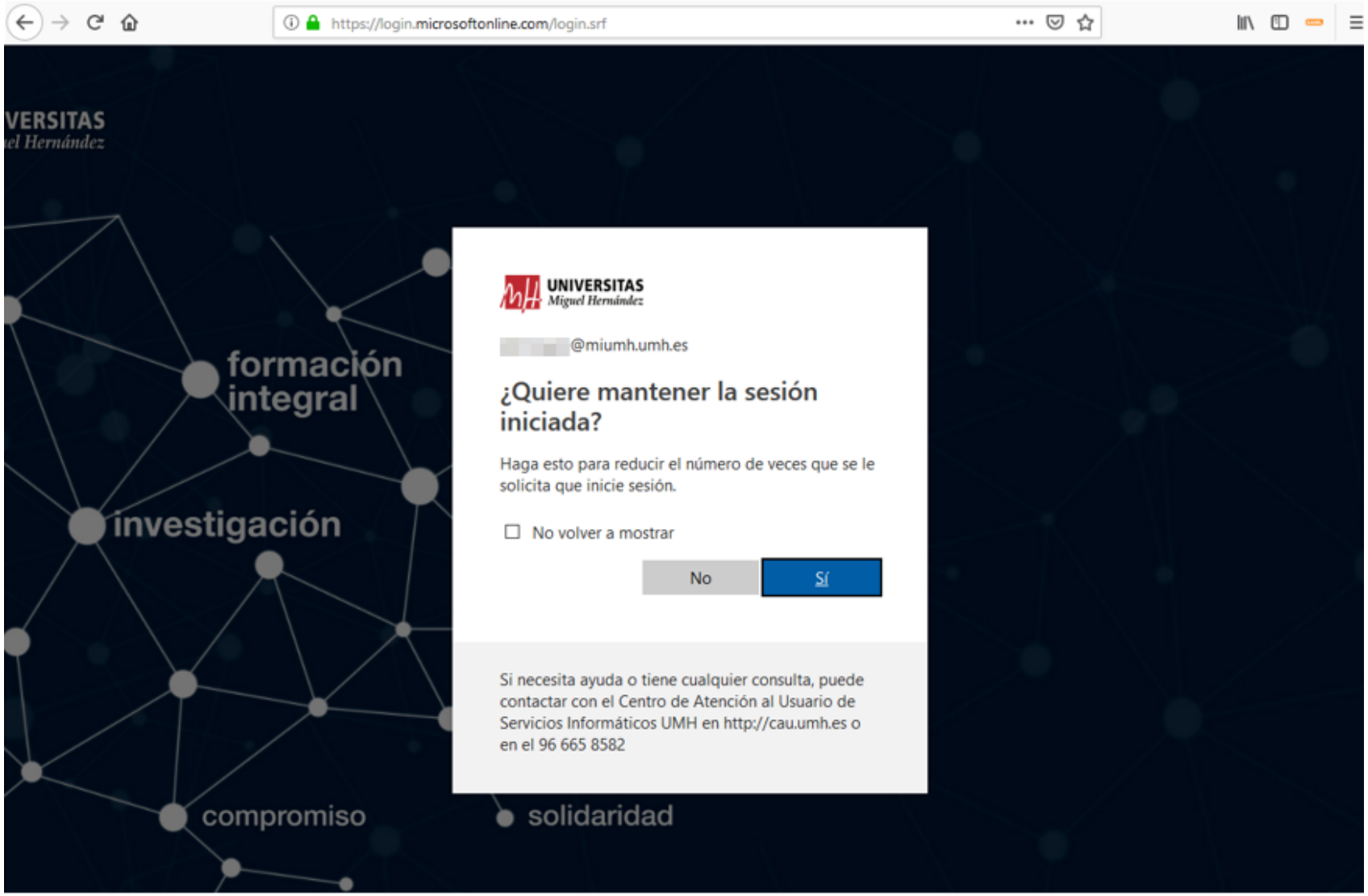


UNIVERSITAS
Miguel Hernández

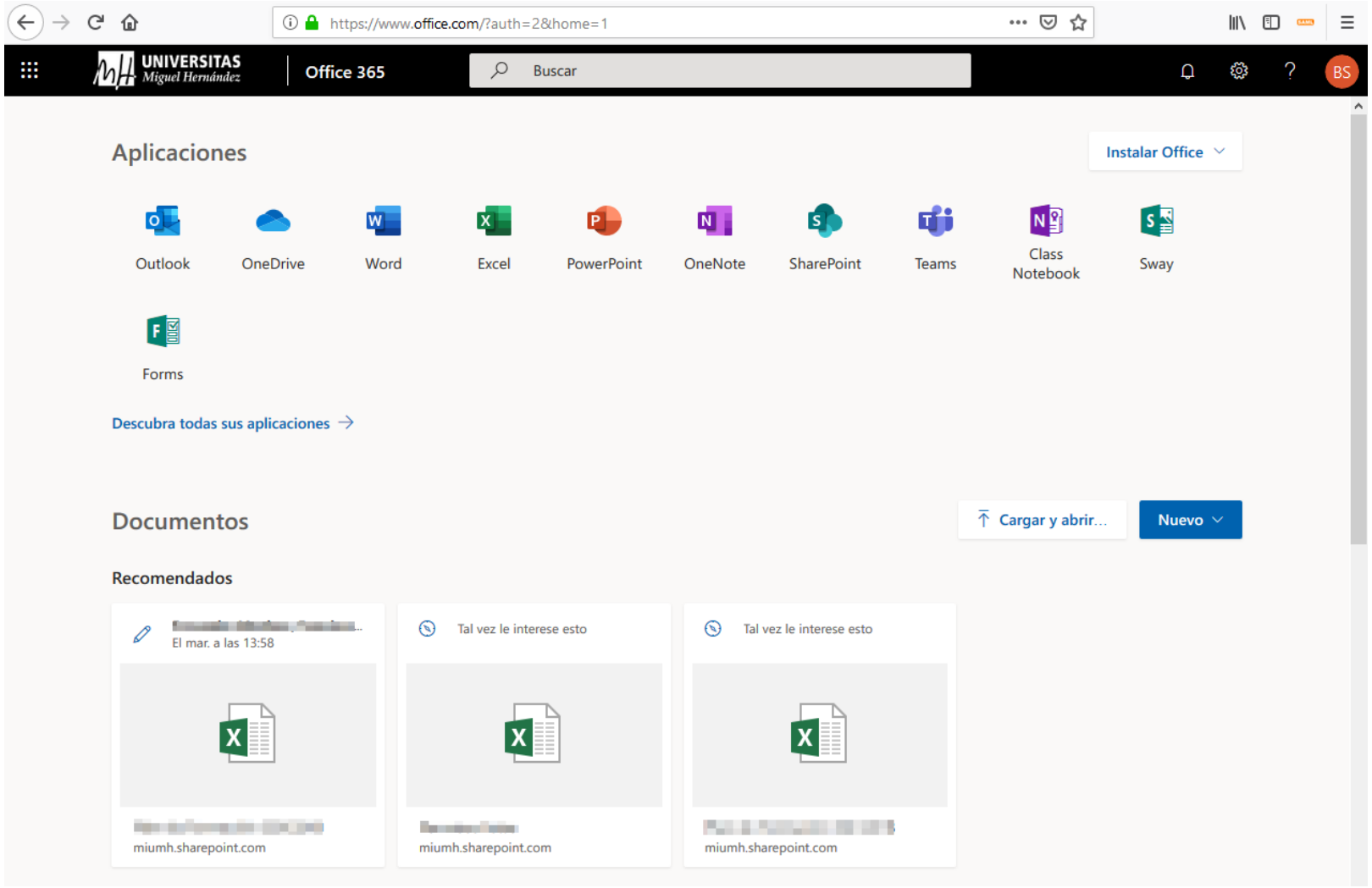
Accediendo a través de https://portal.miumh.umh.es



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



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

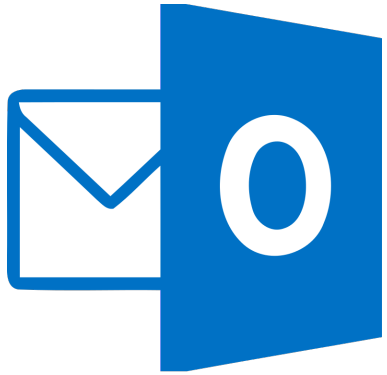


UNIVERSITAS Miguel Hernández

UNIVERSITAS Miguel Hernández

Clientes de correo de escritorio

Microsoft Outlook: Exchange Web Services (EWS)

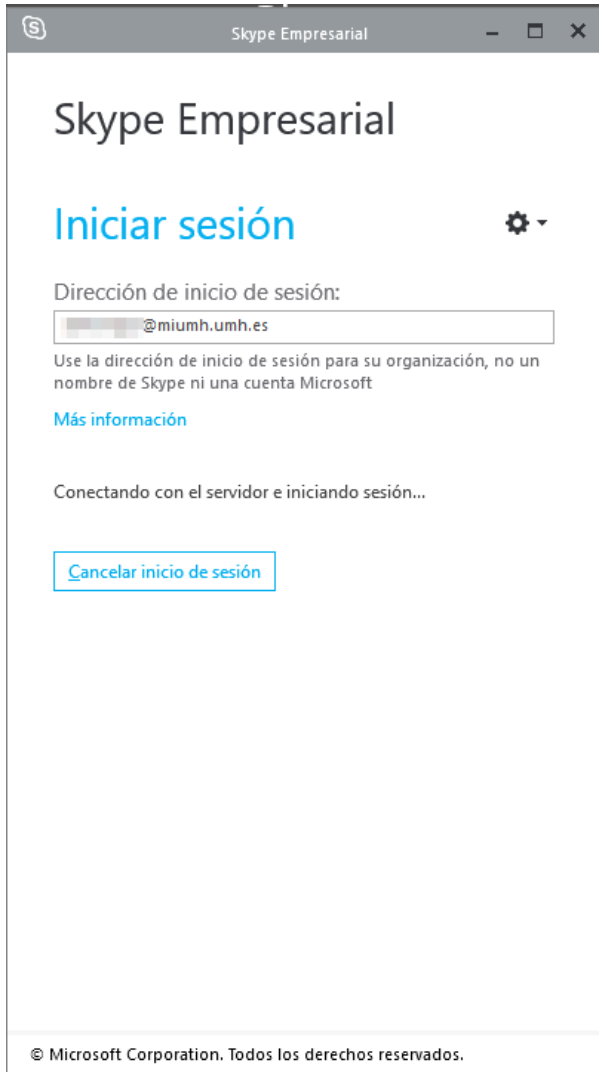


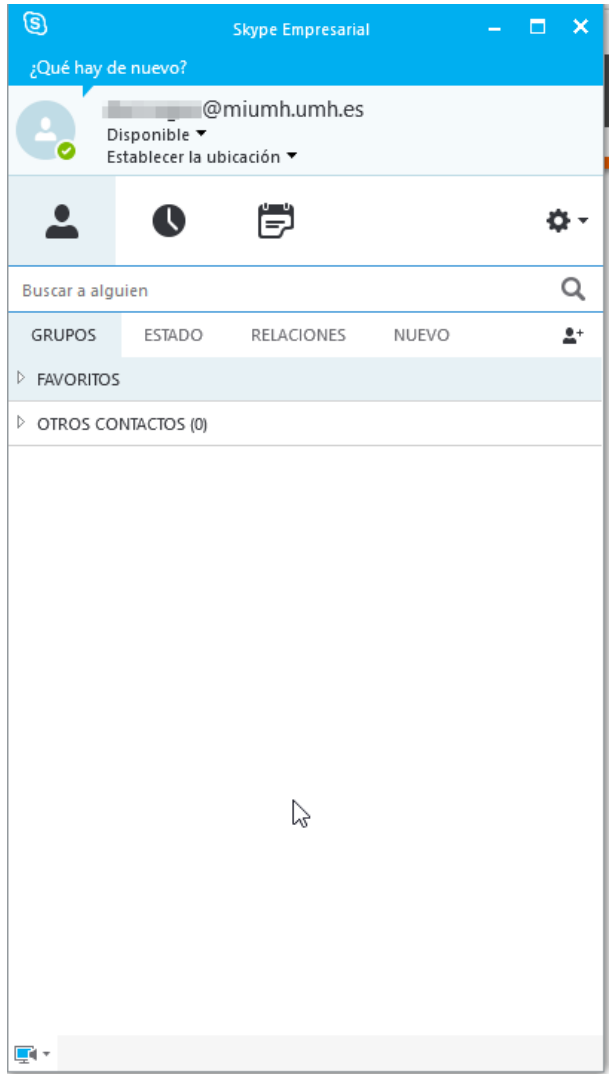
Mozilla Thunderbird: IMAP

Evolution: Exchange Web Services (EWS)

UNIVERSITAS Miguel Hernández

Skype empresarial





UNIVERSITAS Miguel Hernández

Configuración en adas

Agregar metadatos de Microsoft.

Crear los atributos:

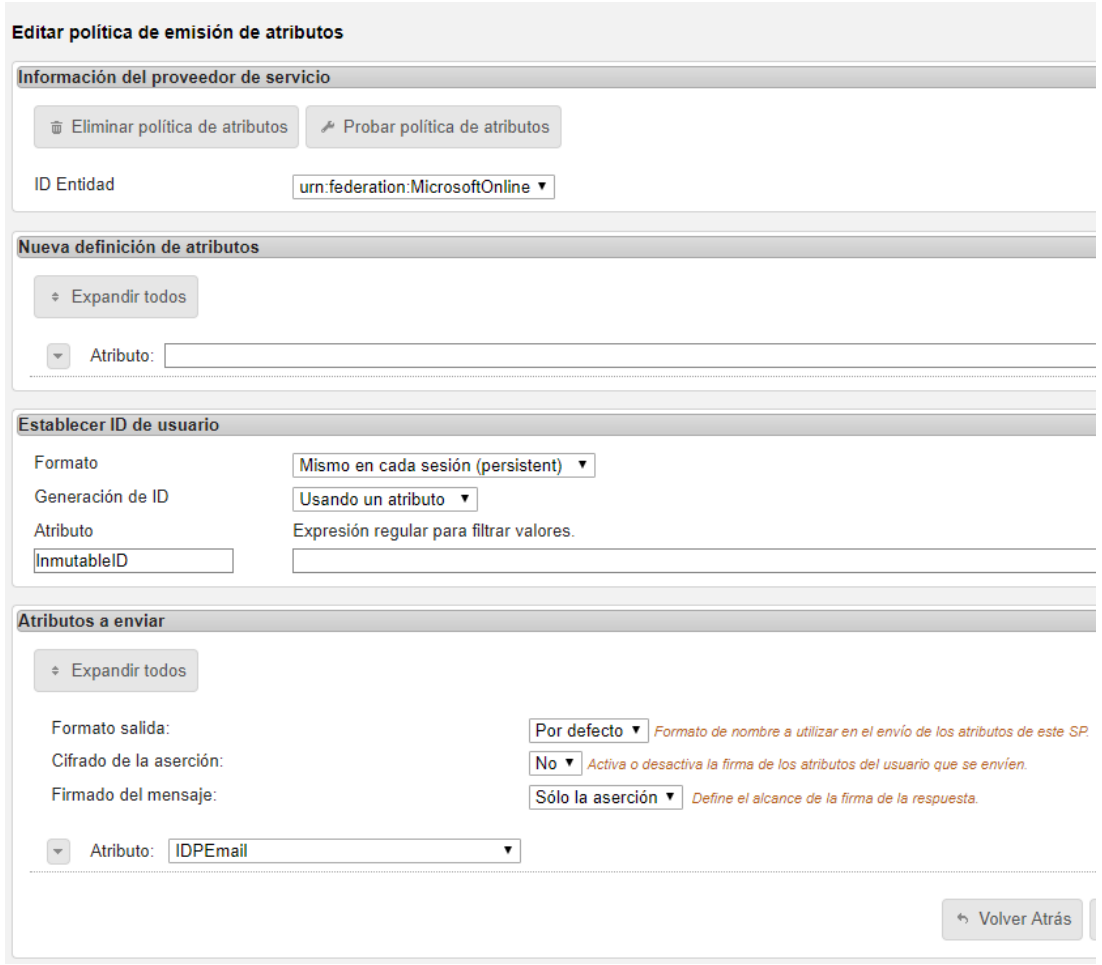
- ImmutableID
- IDPEmail

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



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]98d88</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]s@miumh.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>[redacted]=</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>[redacted]</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:X509Data>
                            <ds:X509Certificate>[redacted]</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">18d93[redacted]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">sbriongos@miumh.umh.es</saml:AttributeValue>
                    </saml:Attribute>
                </saml:AttributeStatement>
            </saml:Assertion>
        </samlp:Response>
```

Desarrollos

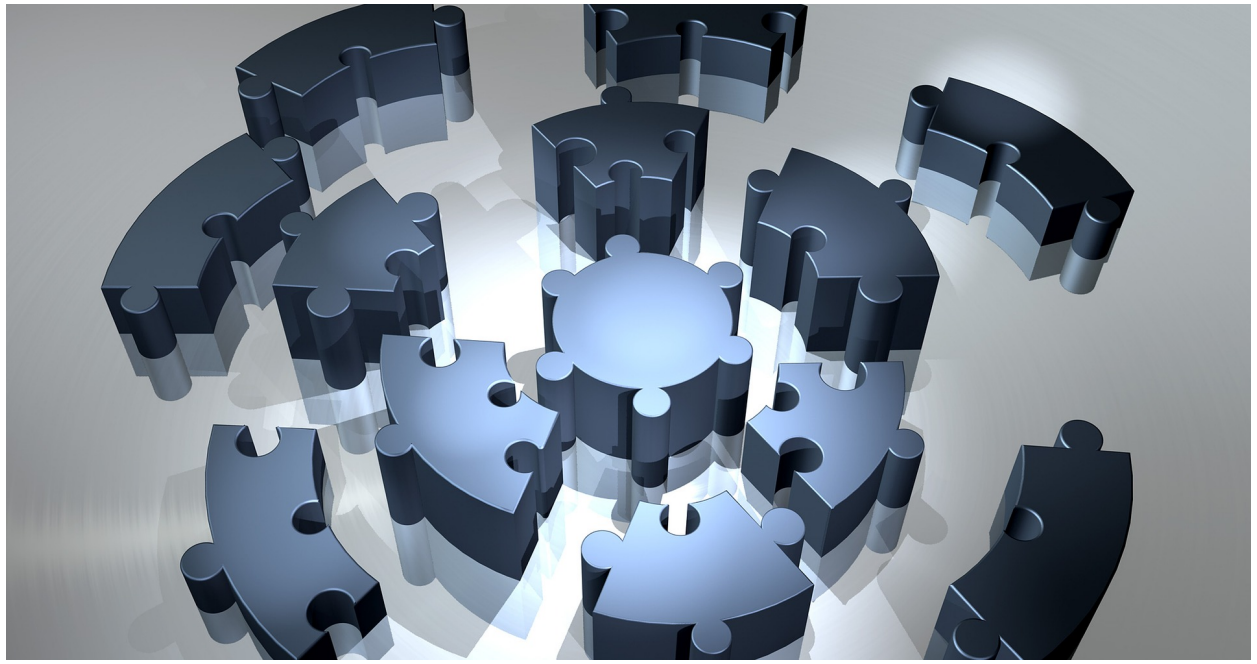
Scripts powershell para:

- 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.



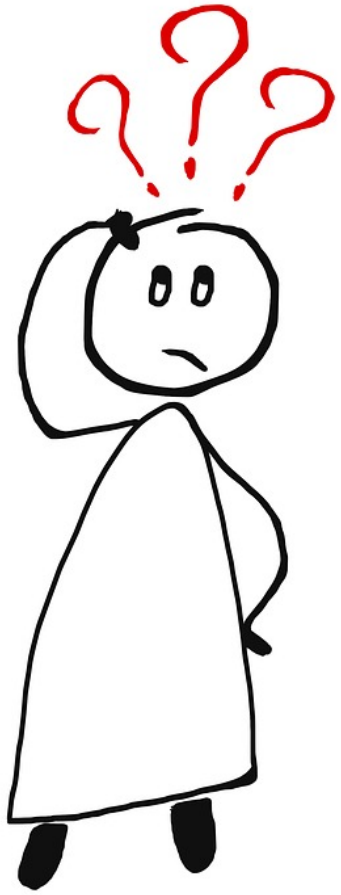
Más información y dudas…

Más información y dudas…

Gracias.

Sergio Briongos Caballero
sbriongos@umh.es

UNIVERSITAS Miguel Hernández



UNIVERSITAS Miguel Hernández