cl@ve y Office 365 vía SIR2

José Manuel Macías <jmanuel.macias@rediris.es>

Valencia, 15 de noviembre de 2015

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
red.es
RedIRIS

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
red.es
RedIRIS

cl@ve en SIR2: requisitos

- Universidades públicas del SUE
- Servicios de cara al ciudadano que requieran autenticación
  - no se contempla por ahora el caso de autenticación de usuarios propios para otros servicios no destinados a ciudadanos
- Se detallan en:

  https://www.rediris.es/sir2/cl@ve/

Cl@ve en SIR2: la pasarela

- Dos entornos: pruebas (`clave-pre`) y producción (`clave`)
- Admite dos modos de funcionamiento:
  - Con extensiones STORK
  - Perfil SAML 2.0 WebSSO
- El flujo de trabajo:
  - Pruebas → Solicitud → Producción
- En el paso a producción sólo cambian:
  - *end-points* SAML (URLs a las que se envían las peticiones)
  - Certificado con el que viene firmada la aserción de atributos
    - No cambia el certificado con el que se firma la respuesta

Cl@ve en SIR2: Procedimiento de alta

- Comprobar elegibilidad
- Desplegar un proveedor de servicio
  - Guía de configuración y ejemplos (tanto de MINHAP como en wiki de SIR2)
  - Solicitar (correo a sir2@rediris.es) conexión al entorno de pruebas
- Una vez realizadas las pruebas, solicitar adhesión al servicio en producción
- El proveedor se configura con la información proporcionada en producción

Cl@ve en SIR2: Recursos

- Se reutilizan buena parte de los recursos de SIR2:
  - De cara a SIR2 es un perfil tecnológico de la federación:
    - `http://www.rediris.es/sir2/politica/#perfiles-tecnologicos`
    - Esto implica haber comenzado la migración a SIR2
      - Aclarar que no se obliga a tener ya desplegado un IdP SAML2int
  - Coordinación a través de la lista SIR-users
  - Contacto (helpdesk)
    - Correo a sir2@rediris.es
    - O a través de formulario de contacto:

      `http://www.rediris.es/ayuda/contact.php?contact=sir2`
  - Documentación y ejemplos en wiki de SIR2:

    `http://wiki.rediris.es/SIR2/Perfil_tecnologico_Cl@ve`
- Validación de Condiciones de uso a través de herramienta conectada a SIR2

Cl@ve en SIR2: Validación de solicitudes

- La solicitud la realiza un técnico de la institución
  - Nombre (`displayName` o `dispN`) y dirección de correo electrónico (`mail`)
  - Además, el técnico ha de que proporcionar tres detalles:
    - Código DIR3 de la unidad orgánica
    - Nombre del procedimiento / Código SIA
    - URL de entrada al procedimiento
- El PER (Persona de Enlace con RedIRIS) de la institución valida la solicitud
- El responsable del servicio valida los datos, confirmando la adhesión
- Toda la información y fechas se recogen en un documento

Cl@ve en SIR2: Validación de solicitudes

Paso 1: Responsable técnico
solicita el acceso

SIR2

Validación de condiciones de uso para SPs cl@ve

1 Solicitud — Responsable Técnico
2 Validación — Persona de enlace con RedIRIS
3 Aprobación — Responsable del servicio

Solicitud del servicio

Está a punto de solicitar su adhesión al servicio **'Federación SIR2 · Proveedor de Servicio cl@ve'**.

Se muestran los parámetros que han sido obtenidos de su proveedor de identidad y que serán incluidos en el documento de solicitud:

- **Persona solicitante:** Jose Manuel Macias Luna
- **Correo electrónico:** jmanuel.macias@rediris.es
- **Dominio de la institución:** rediris.es

Además, deberá confirmar los siguientes datos adicionales:

Código DIR3 de la organización:

Nombre de la aplicación:

(ha de ser un nombre descriptivo, por ejemplo: Sede electrónica de la Universidad Autónoma de Madrid)

URL principal del servicio que se desea añadir:

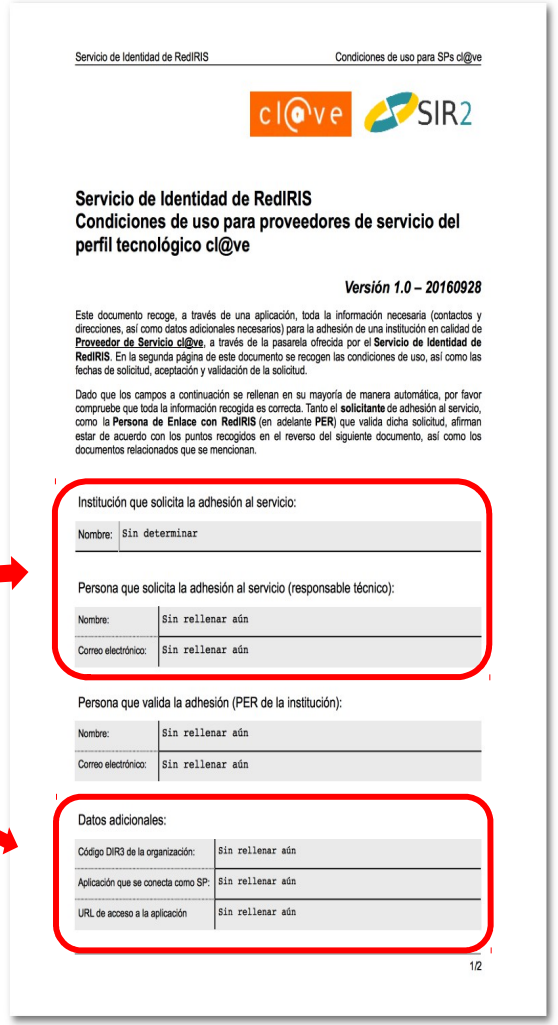
(por ejemplo: https://sede.uam.es/)

En el paso siguiente se mostrará el documento que recogerá toda esta información, y se le pedirá confirmación. Dicho documento será enviado al responsable en tu organización, el cual validará esta solicitud en la **fase 2**.

SOLICITAR

Datos solicitante y organización recogidos vía SIR2

Datos adicionales y del proveedor de servicio



Servicio de Identidad de RedIRIS — Condiciones de uso para SPs cl@ve

cl@ve SIR2

Servicio de Identidad de RedIRIS
Condiciones de uso para proveedores de servicio del perfil tecnológico cl@ve

Versión 1.0 – 20160928

Este documento recoge, a través de una aplicación, toda la información necesaria (contactos y direcciones, así como datos adicionales necesarios) para la adhesión de una institución en calidad de **Proveedor de Servicio cl@ve**, a través de la pasarela ofrecida por el **Servicio de Identidad de RedIRIS**. En la segunda página de este documento se recogen las condiciones de uso, así como las fechas de solicitud, aceptación y validación de la solicitud.

Dado que los campos a continuación se rellenan en su mayoría de manera automática, por favor compruebe que toda la información recogida es correcta. Tanto el **solicitante** de adhesión al servicio, como la **Persona de Enlace con RedIRIS** (en adelante **PER**) que valida dicha solicitud, afirman estar de acuerdo con los puntos recogidos en el reverso del siguiente documento, así como los documentos relacionados que se mencionan.

Institución que solicita la adhesión al servicio:

Nombre:	Sin determinar

Persona que solicita la adhesión al servicio (responsable técnico):

Nombre:	Sin rellenar aún
Correo electrónico:	Sin rellenar aún

Persona que valida la adhesión (PER de la institución):

Nombre:	Sin rellenar aún
Correo electrónico:	Sin rellenar aún

Datos adicionales:

Código DIR3 de la organización:	Sin rellenar aún
Aplicación que se conecta como SP:	Sin rellenar aún
URL de acceso a la aplicación	Sin rellenar aún

1/2

Cl@ve en SIR2: Validación de solicitudes

Paso 2: Un PER de la Universidad valida la solicitud

SIR2

Validación de condiciones de uso para SPs cl@ve

1 Solicitud — Responsable Técnico

2 Validación — Persona de enlace con RedIRIS

3 Aprobación — Responsable del servicio

Validación de adhesión al servicio

Las siguientes pantallas le permiten aprobar, como responsable de su institución, la solicitud de alta al servicio **Federación SIR2 · Proveedor de Servicio cl@ve.**

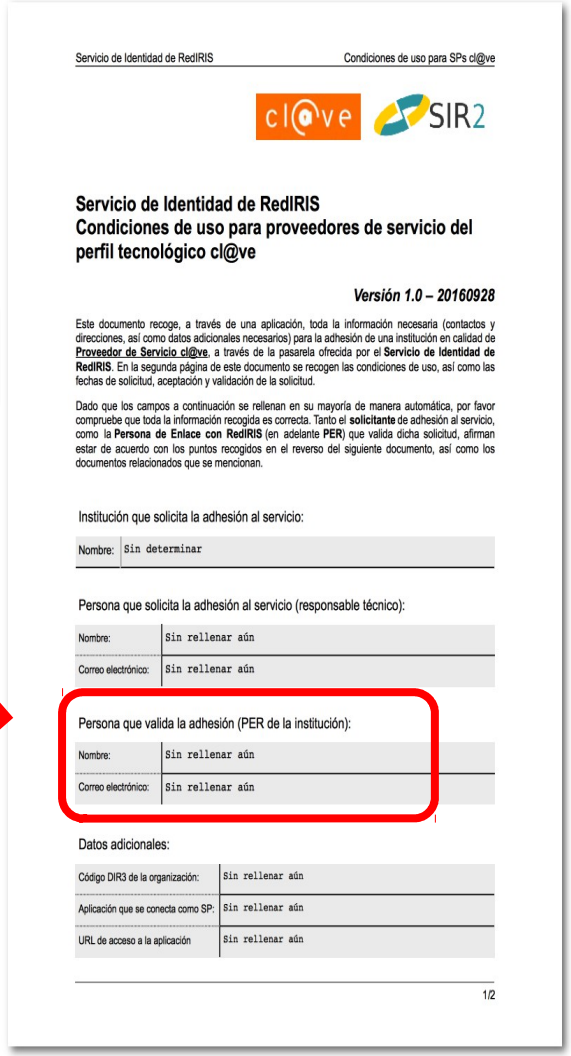
Se muestran los parámetros que han sido obtenidos de su proveedor de identidad y que serán incluidos en el documento de solicitud antes de su aprobación:

- **Persona que valida:** Jose Manuel Macias Luna
- **Correo electrónico:** jmanuel.macias@rediris.es

En el paso siguiente se mostrará el documento que recogerá toda esta información, y se le pedirá confirmación. Dicho documento será enviado al responsable para su comprobación, el cual dará el visto bueno en la **fase 3**.

VALIDAR

Datos del PER de la Universidad



Servicio de Identidad de RedIRIS — Condiciones de uso para SPs cl@ve

cl@ve SIR2

Servicio de Identidad de RedIRIS
Condiciones de uso para proveedores de servicio del perfil tecnológico cl@ve

Versión 1.0 – 20160928

Este documento recoge, a través de una aplicación, toda la información necesaria (contactos y direcciones, así como datos adicionales necesarios) para la adhesión de una institución en calidad de **Proveedor de Servicio cl@ve**, a través de la pasarela ofrecida por el **Servicio de Identidad de RedIRIS**. En la segunda página de este documento se recogen las condiciones de uso, así como las fechas de solicitud, aceptación y validación de la solicitud.

Dado que los campos a continuación se rellenan en su mayoría de manera automática, por favor compruebe que toda la información recogida es correcta. Tanto el **solicitante** de adhesión al servicio, como la **Persona de Enlace con RedIRIS** (en adelante **PER**) que valida dicha solicitud, afirman estar de acuerdo con los puntos recogidos en el reverso del siguiente documento, así como los documentos relacionados que se mencionan.

Institución que solicita la adhesión al servicio:

Nombre:	Sin determinar

Persona que solicita la adhesión al servicio (responsable técnico):

Nombre:	Sin rellenar aún
Correo electrónico:	Sin rellenar aún

Persona que valida la adhesión (PER de la institución):

Nombre:	Sin rellenar aún
Correo electrónico:	Sin rellenar aún

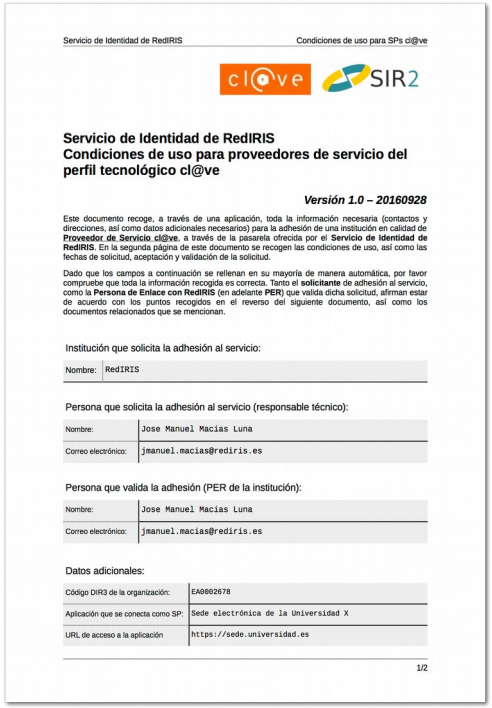
Datos adicionales:

Código DIR3 de la organización:	Sin rellenar aún
Aplicación que se conecta como SP:	Sin rellenar aún
URL de acceso a la aplicación	Sin rellenar aún

1/2

Cl@ve en SIR2: Validación de solicitudes

Paso 3: El responsable del servicio aprueba la solicitud y se genera un documento final



Servicio de Identidad de RedIRIS — Condiciones de uso para SPs cl@ve

cl@ve SIR2

Servicio de Identidad de RedIRIS
Condiciones de uso para proveedores de servicio del perfil tecnológico cl@ve

Versión 1.0 – 20160928

Este documento recoge, a través de una aplicación, toda la información necesaria (contactos y direcciones, así como datos adicionales necesarios) para la adhesión de una institución en calidad de **Proveedor de Servicio cl@ve**, a través de la pasarela ofrecida por el **Servicio de Identidad de RedIRIS**. En la segunda página de este documento se recogen las condiciones de uso, así como las fechas de solicitud, aceptación y validación de la solicitud.

Dado que los campos a continuación se rellenan en su mayoría de manera automática, por favor compruebe que toda la información recogida es correcta. Tanto el **solicitante** de adhesión al servicio, como la **Persona de Enlace con RedIRIS** (en adelante **PER**) que valida dicha solicitud, afirman estar de acuerdo con los puntos recogidos en el reverso del siguiente documento, así como los documentos relacionados que se mencionan.

Institución que solicita la adhesión al servicio:

Nombre:	RedIRIS

Persona que solicita la adhesión al servicio (responsable técnico):

Nombre:	Jose Manuel Macias Luna
Correo electrónico:	jmanuel.macias@rediris.es

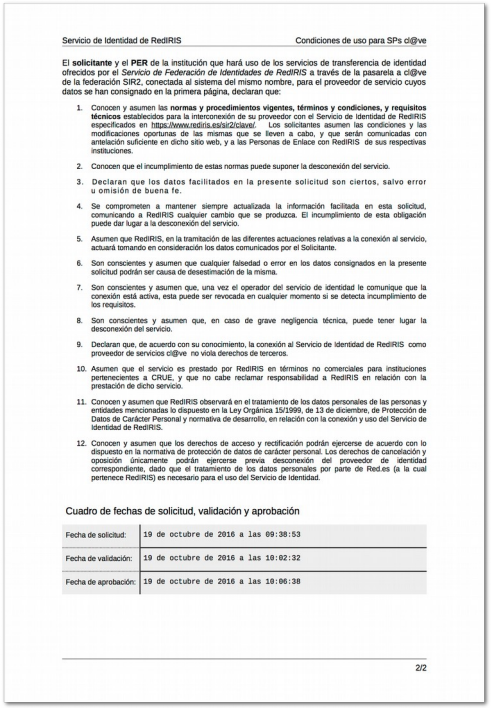
Persona que valida la adhesión (PER de la institución):

Nombre:	Jose Manuel Macias Luna
Correo electrónico:	jmanuel.macias@rediris.es

Datos adicionales:

Código DIR3 de la organización:	EA0002678
Aplicación que se conecta como SP:	Sede electrónica de la Universidad X
URL de acceso a la aplicación	https://sede.universidad.es

1/2



Servicio de Identidad de RedIRIS — Condiciones de uso para SPs cl@ve

El **solicitante** y el **PER** de la institución que hará uso de los servicios de transferencia de identidad ofrecidos por el *Servicio de Federación de Identidades de RedIRIS* a través de la pasarela a cl@ve de la federación SIR2, conectada al sistema del mismo nombre, para el proveedor de servicio cuyos datos se han consignado en la primera página, declaran que:

1. Conocen y asumen las **normas y procedimientos vigentes, términos y condiciones, y requisitos técnicos** establecidos para la interconexión de su proveedor con el Servicio de Identidad de RedIRIS especificados en https://www.rediris.es/sir2/clave/. Los solicitantes asumen las condiciones y las modificaciones oportunas de las mismas que se lleven a cabo, y que serán comunicadas con antelación suficiente en dicho sitio web, y a las Personas de Enlace con RedIRIS de sus respectivas instituciones.
2. Conocen que el incumplimiento de estas normas puede suponer la desconexión del servicio.
3. Declaran que los datos facilitados en la presente solicitud son ciertos, salvo error u omisión de buena fe.
4. Se comprometen a mantener siempre actualizada la información facilitada en esta solicitud, comunicando a RedIRIS cualquier cambio que se produzca. El incumplimiento de esta obligación puede dar lugar a la desconexión del servicio.
5. Asumen que RedIRIS, en la tramitación de las diferentes actuaciones relativas a la conexión al servicio, actuará tomando en consideración los datos comunicados por el Solicitante.
6. Son conscientes y asumen que cualquier falsedad o error en los datos consignados en la presente solicitud podrán ser causa de desestimación de la misma.
7. Son conscientes y asumen que, una vez el operador del servicio de identidad le comunique que la conexión está activa, esta puede ser revocada en cualquier momento si se detecta incumplimiento de los requisitos.
8. Son conscientes y asumen que, en caso de grave negligencia técnica, puede tener lugar la desconexión del servicio.
9. Declaran que, de acuerdo con su conocimiento, la conexión al Servicio de Identidad de RedIRIS como proveedor de servicios cl@ve no viola derechos de terceros.
10. Asumen que el servicio es prestado por RedIRIS en términos no comerciales para instituciones pertenecientes a CRUE, y que no cabe reclamar responsabilidad a RedIRIS en relación con la prestación de dicho servicio.
11. Conocen y asumen que RedIRIS observará en el tratamiento de los datos personales de las personas y entidades mencionadas lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, en relación con la conexión y uso del Servicio de Identidad de RedIRIS.
12. Conocen y asumen que los derechos de acceso y rectificación podrán ejercerse de acuerdo con lo dispuesto en la normativa de protección de datos de carácter personal. Los derechos de cancelación y oposición únicamente podrán ejercerse previa desconexión del proveedor de identidad correspondiente, dado que el tratamiento de los datos personales por parte de Red.es (a la cual pertenece RedIRIS) es necesario para el uso del Servicio de Identidad.

Cuadro de fechas de solicitud, validación y aprobación

Fecha de solicitud:	19 de octubre de 2016 a las 09:38:53
Fecha de validación:	19 de octubre de 2016 a las 10:02:32
Fecha de aprobación:	19 de octubre de 2016 a las 10:06:38

2/2

- El documento final es un «resguardo» de la solicitud
- Solicitante y persona que aprueban pueden ver en cada momento la información que se va recogiendo
- Recoge la información de contacto y básica de funcionamiento
- Se recogen las fechas de solicitud, validación y confirmación
- El documento va firmado con un certificado de Digicert

Cl@ve en SIR2: Estado actual

- Acuerdo entre CRUE y MINHAP firmado
- Pasarela de producción desplegada y configurada
  - Ningún SP conectado a día de hoy, a la espera de conexión en de la pasarela desde la plataforma cl@ve
- RedIRIS ha licitado el prepago de SMSs para retos lanzados mediante este sistema desde AEAT y Seg. Social
- Procedimientos listos
- Documentación prácticamente lista
- Varias universidades a la espera de incorporarse, que esperamos puedan comenzar a hacerlo en los próximos días o semanas

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
red.es
RedIRIS

Office365 vía SIR2: Piloto

- Idea que se persigue:
  - homogeneizar el acceso a Office365, usando la federación SIR2 para ello
  - Facilitar el aprovisionamiento de usuarios
  - Estudiar viabilidad de accesos no web
- ¿cómo es de lo contrario?
  - Dos posibilidades:
    - Sincronización de datos con Microsoft
    - O bien, añadir determinados servicios en nuestra infraestructura + IdP SAML con mapeo de atributos (o «claims») a los esperados por Microsoft
- La alternativa:
  - Aprovisionamiento vía **portal de aprovisionamiento**
  - Acceso federado SAML con conversión de atributos en SIR2

Office365 vía SIR2: Estado actual

- Fase inicial del piloto con la Universidad de Sevilla
- Acuerdo de atributos a intercambiar
- Desarrollo de portal de aprovisionamiento
  - En estos momentos se está procediendo a su despliegue
- Tan pronto esté el despliegue, se va a ampliar el piloto a varias universidades
- El uso de protocolos no web, se deja de lado de momento
  - Inicialmente sólo se soporta Web-SSO

Office365 vía SIR2: Atributos

- Perfil administrador de NREN:
- `sHO` + `eduPersonEntitlement`
- Perfil administrador de organización:
- `sHO` + `eduPersonEntitlement`
  - Valor: `urn:mace:rediris.es:entitlement:sir2:o365:org-admin`
- Usuario realizando el aprovisionamiento:
  - Identificador de correo
    - Hemos acordado poder utilizar `mail` o `irisMailMainAddress`
      - `mail` presenta el problema de que puede ser multivaluado: tiene que ser un valor único
  - Identificador de pertenencia a grupos (dos posibilidades):
    - `eduPersonAffiliation` → grupos (staff, student, ...)
    - `eduPersonEntitlement` → prefijo (urn) + valor de grupo

Office365 vía SIR2: Flujo aproximado

1) Institución solicita el acceso
2) RedIRIS añade a institución en portal de aprovisionamiento
3) RedIRIS añade mapeos de atributos en hub de SIR2
4) Administrador de institución configura parámetros de institución:
   - Branding
   - Mapeos de atributos
   - Grupos/Perfiles de usuarios y licencias a activar
   - Posibilidad de preaprovisionamiento
5) Administrador de institución configura su tenant con parámetros para acceso vía SIR2
6) Usuarios acceden al portal de aprovisionamiento una vez
7) Portal de aprovisionamiento, aprovisiona cuentas en función de atributos definidos
8) Usuario accede al portal de Office365 con sso de su organización