

# **Condiciones de uso del Servicio de Certificados Digitales**

## **1. Objeto**

Este documento describe las condiciones de uso del Servicio de Certificados Digitales (*“Trusted Certificate Service”*, TCS, por sus siglas en inglés).

El Servicio se presta a través de Rediris, gracias a acuerdos de GÉANT (Asociación de Redes Académicas Europeas) con operadores de certificación. Cualquier cambio en estos acuerdos afectarán a estas condiciones de uso. La UJA podrá modificar estas condiciones para reflejar cambios en el Servicio, informando a todos los usuarios del mismo.

El usuario, al utilizar el Servicio, acepta estas condiciones.

## **2. Ámbito de aplicación**

Los certificados digitales deben usarse exclusivamente para el acceso a recursos propios de la Universidad de Jaén (UJA), en particular para actividades académicas y de investigación.

Estas condiciones se refieren a todos los certificados digitales, con independencia de su tipo.

## **3. Servicios**

Este servicio permite la solicitud, renovación y/o revocación de los siguientes tipos de certificados digitales:

- Certificados SSL de servidor, con nombres de dominio ujaen.es: se utilizan para establecer una conexión cifrada entre el servidor web y el navegador del usuario. Hay muchas razones para instalar un certificado SSL: seguridad (la mayoría de navegadores alertan cuando un sitio web no es seguro), posicionamiento web, etc..
- Certificados de firma de código (CS, *Code Signing*) en la Universidad de Jaén: se utilizan para demostrar que un programa o código desarrollado no ha sido alterado por terceras personas.

## **4. Usuarios y requisitos**

Podrá solicitar este Servicio el PAS y PDI de la Universidad de Jaén.

El usuario se encargará de generar el par de claves (pública y privada). Posteriormente enviará al Servicio de Informática de la UJA el archivo de solicitud de firma de certificado (CSR) a través de una petición Murphy. Una vez verificados todos los datos, se emitirá el certificado.

Todos los certificados tienen fecha de caducidad. El usuario deberá solicitar la renovación antes de que finalice el periodo de validez.

## **5. Soporte**

El usuario es responsable de la instalación del certificado, así como del mantenimiento de los equipos o sistemas que los utilicen.

El Servicio de Informática ofrecerá un soporte “de mejor esfuerzo”, escalando a la autoridad de certificación aquellas incidencias que no pueda resolver.

## **6. Medidas de seguridad y revocación**

El usuario es responsable de la custodia de la clave privada asociada al certificado, debiendo preservar su confidencialidad y aplicar medidas de seguridad para protegerla frente a su posible revelación. Si el

usuario sospecha de un uso fraudulento del certificado o revelación de la clave privada, deberá solicitar su revocación, en el plazo de un día hábil, contado a partir de la fecha de la incidencia.

La UJA podrá revocar el certificado digital en los siguientes supuestos:

- La clave privada asociada al certificado se ha revelado o se ha puesto en peligro.
- El certificado no se ha usado para los fines previstos
- Incumplimiento de los prácticas o procedimientos descritos en los acuerdos [Trusted Certificated Service de Rediris](#) o de la autoridad de certificación.
- Incumplimiento de estas normas o de la legislación vigente

Por su parte, y en cualquier momento, si el Usuario no desea continuar utilizando el Servicio de Certificados Digitales, se encuentra facultado para solicitar su revocación.