



# Custodia y gestión centralizada de los certificados digitales



**redtrust**  
a KEYFACTOR company

# Agenda

---



- 1 Sobre **Redtrust**
- 2 Problemática del uso de los certificados digitales sin gestión
- 3 Cómo ayuda **Redtrust** a las empresas a controlar y gestionar sus certificados
- 4 Consola de Administración de **Redtrust**
- 5 Creación de Políticas de uso y Auditoría
- 6 Uso de **Redtrust** por el usuario final
- 7 Modalidades de servicio **Redtrust**
- 8 Clientes





# Sobre Redtrust

*Gestor de certificados digitales para garantizar  
el máximo control y seguridad*

# Sobre Redtrust

---



Redtrust es la solución autocontenida para la **gestión centralizada de los certificados digitales**, permitiendo almacenarlos todos en un único repositorio, establecer políticas de uso y obtener una auditoría detallada para saber quién, cuándo y para qué se ha utilizado cada certificado.

Redtrust posibilita un total cumplimiento corporativo y legal del ciclo de vida de los certificados digitales en las organizaciones, asegurando y previniendo contra riesgos externos e internos, además de reducir drásticamente el coste y esfuerzo requeridos para su correcta gestión.

Redtrust cuenta con un equipo de expertos con más de 15 años de experiencia en el área de la seguridad de la información, que siempre busca nuevos retos en las necesidades de sus clientes y sus partners.





# Problemática certificados

*Ausencia de gestión y control sobre los  
certificados digitales*

# Problemática con el uso de certificados digitales



¿Qué ocurre cuando NO SE GESTIONAN NI CONTROLAN los certificados digitales?



## Indisponibilidad

La indisponibilidad de un certificado causa interrupción del trabajo y la interrupción de la actividad.



## Suplantación de identidad

El robo o acceso no legítimo a un certificado tiene consecuencias impredecibles y negativas, como la suplantación de identidad.



## Sin monitorización

Los certificados que están siendo utilizados no pueden ser auditados, desconociendo quién los usa y qué se hace con ellos.



## Sin limitaciones

No es posible establecer políticas para limitar los usos del certificado: cualquier usuario puede usar un certificado en nombre del propietario, sin ningún control.



## Almacenamiento inseguro

Los certificados instalados en un equipo representan un riesgo para el propietario y la compañía: pueden ser copiados, exportados, robados...



## Costes

La renovación de los certificados por pérdidas o por caducidad es costosa, así como la cantidad de personal destinado a instalar los certificados duplicados.



## Confidencialidad

La información confidencial está expuesta si no se cuenta con un sistema centralizado con políticas de seguridad y mecanismos de control.

# Problemática con el uso de certificados digitales



¿Cuál es la NECESIDAD de las empresas?



Las organizaciones se enfrentan a un importante reto: **proteger**, **gestionar**, **controlar** y, por tanto, **optimizar** el uso de sus certificados digitales



# Beneficios Redtrust

*Cómo ayuda Redtrust en la gestión y el control de los certificados digitales*



# Beneficios Redtrust



Podemos agrupar los beneficios de implementar Redtrust para la gestión de los certificados digitales en 3 grandes bloques:

## CONTROL

- ¿**Quién** utiliza los certificados de empresa?
- ¿**Cómo** se utilizan los certificados?
- ¿**Dónde** se utilizan estos certificados?
- ¿**Para** qué se utilizan los certificados?

## GESTIÓN

- Almacenamiento
- Transporte
- Utilización
- Supervisión
- Recuperación
- Revocación

## PROTECCIÓN

- **Evitar** la indisponibilidad de los certificados
- **Impedir** el uso indebido de un certificado
- **Proteger** contra robos y ataques

# Beneficios Redtrust



# Beneficios Redtrust



¿Cómo ayuda **Redtrust** en el control y gestión de los certificados digitales?



## Emisión de certificados desde Redtrust

- ▶ Emisión de certificados sin interaccionar con las páginas de la FNMT y con las claves creadas en Redtrust.
- ▶ Sin necesidad de configurar el navegador y con acceso desde cualquier dispositivo.
- ▶ Posibilidad de constituirse como Autoridad de Registro (RA) para la emisión de certificados, de forma online, de la CA Firmaprofesional.



## Centralización de certificados

- ▶ Todos los certificados en un repositorio único, controlado y seguro.
- ▶ Los certificados dejan de estar distribuidos sin control en los equipos informáticos: ya no se encuentran instalados en cada uno de esos equipos.
- ▶ La centralización permite a los usuarios acreditar su identidad desde cualquier lugar y momento.



## Establecimiento de políticas de uso

- ▶ El acceso de los certificados puede ser limitado a los usuarios, así como sobre qué páginas o servicios puede actuar.
- ▶ Posibilidad de autenticación por segundo factor y configuración de control horario.

# Beneficios Redtrust



¿Cómo ayuda **Redtrust** en el control y gestión de los certificados digitales?



## Integración segura y transparente

- ▶ Distribución automática de certificados raíz y de correos electrónicos.
- ▶ Los certificados locales pueden seguir siendo utilizados sin alteraciones.



## Compatible con las soluciones corporativas

- ▶ Integración y compatibilidad con el sistema de credenciales corporativo.
- ▶ Facilidad de registro de eventos en sistemas remotos.



## Auditoría detallada

- ▶ Registro de todas las operaciones realizadas con los certificados.



## Gestión del ciclo de vida

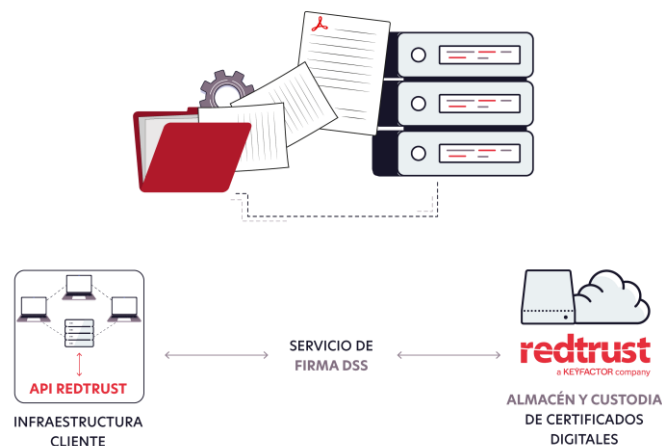
- ▶ Evita tediosas acciones técnicas en cada estación de trabajo para eliminar o introducir nuevos certificados a usuarios.
- ▶ El ciclo completo de la administración del sistema se realiza sobre una única web de administración central.
- ▶ Configuración de alertas de caducidad que notifiquen, con la antelación necesaria, el fin de la vida útil de un certificado.

# Firma digital de documentos con Redtrust



## Firma mediante **DSS** a través de la **API Redtrust**

- Firma documentos con los distintos perfiles XAdES, CAdES y PAdES.
- Automatiza procesos como la firma masiva de documentos.



## Firma a través del módulo de **Signtrust**

- Firma completamente online.
- Desde cualquier dispositivo y navegador web.
- Sin necesidad de software o aplicación de terceros.



## Firma con el resto de **aplicaciones corporativas**

- Firma documentos PDF, PowerPoint, Word o Excel.





# Consola de **Administración**

*Proceso de control de certificados  
digitales y de políticas de usuarios*

# Consola de Administración Redtrust



Tras iniciar sesión en la Consola de Administración se observan 6 pestañas: *Sumario*, *Certificados*, *Alertas*, *Políticas*, *Eventos* y *Acceso*. Desde esta consola podemos administrar los 3 ejes principales de la gestión con Redtrust: los **usuarios**, los **certificados** y el **sistema de políticas de uso**, que conecta los usuarios con los certificados y permite definir qué acciones se autorizan y cuáles no.

## SUMARIO

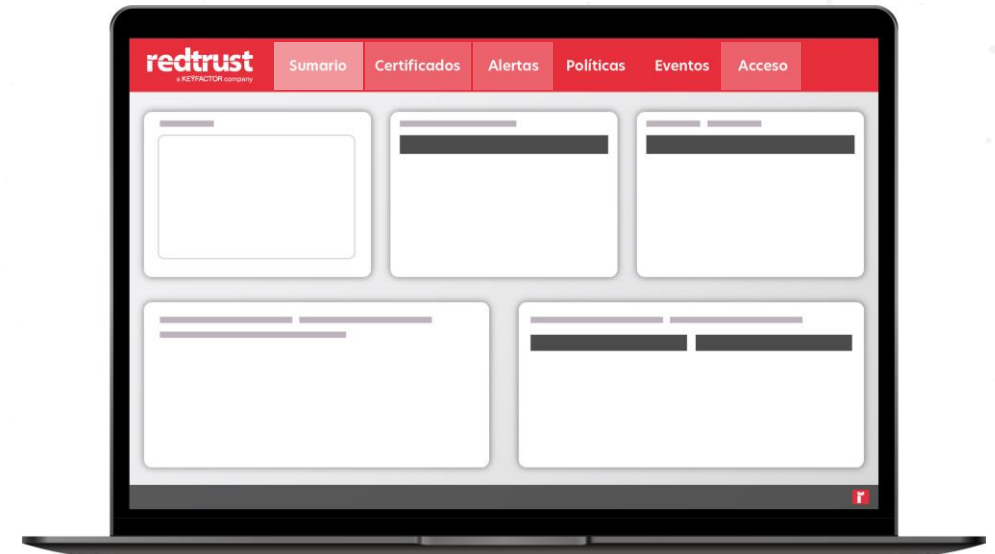
- Últimos eventos.
- Próximos certificados a expirar.
- Certificados expirados.

## CERTIFICADOS

- Alta de nuevos certificados; emisión, renovación.
- Ver certificados: expirados, seleccionados o todos.
- Deshabilitar, eliminar y descargar.
- Agrupar por: políticas, por usuarios, por grupos.

## ALERTAS

- Configuración de alertas: eventos de alertas de caducidad y de usos de los certificados.



## ACCESO

- Usuarios dados de alta en el sistema.
- Dar de alta nuevos usuarios.
- Activar y desactivar certificados.



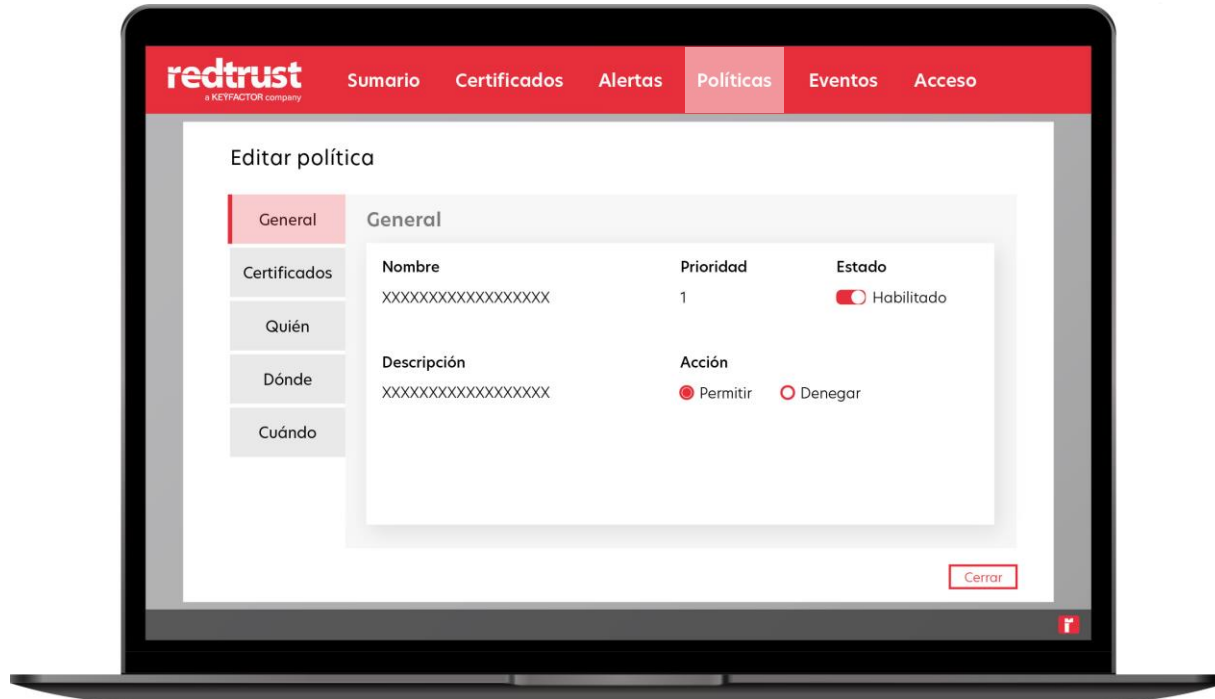


# Políticas de Uso

*Gestión de políticas de uso entre  
usuario y certificados digitales*



# Políticas de **Uso**



Pueden definirse tantas políticas como sean necesarias. En el panel de Políticas vemos: Prioridad, Estado (si está 'Activa o no'), Permisos, Nombre, Certificados (y sus grupos), Usuarios, Rol y Contexto. Cada política se puede 'Editar' y 'Activar'.

- ✓ **GENERAL:** Definimos el nombre de la política, una descripción, le otorgamos una Prioridad antes de activarla y si queremos que sea permisiva o restrictiva.
- ✓ **CERTIFICADOS:** Definimos qué certificados van a intervenir dentro de la política. Se pueden definir tanto uno a uno como por grupos.
- ✓ **QUIÉN:** Definimos qué usuario o usuarios se verán afectados por esta política.
- ✓ **DÓNDE:** Podemos definir aplicaciones que se estén ejecutando tanto en el PC físico como virtual del usuario, así como en las URL donde queremos que actúen estas políticas.
- ✓ **CUÁNDO:** Podemos configurar que esta política actúe siempre o limitar una temporalidad que se adapte a las necesidades.





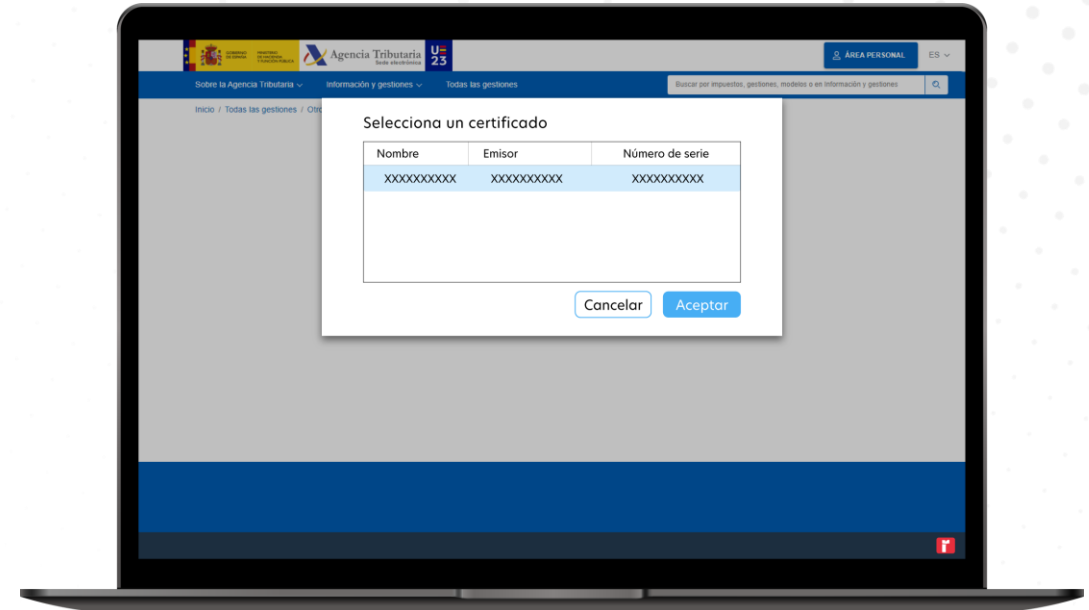
# Uso por el **usuario final**

*La gestión para el usuario final es  
totalmente transparente*

# Uso por el **usuario final**



- ✓ El usuario accede a la web donde quiere hacer una consulta, por ejemplo, en la sede electrónica de la Agencia Tributaria.
- ✓ Al hacer la consulta con certificado electrónico, el explorador indica si ese es el certificado que desea usar. En el momento en el que acepta, **Redtrust** entra en funcionamiento, de forma totalmente transparente para el usuario.
- ✓ El certificado es reconocido y el usuario procede a realizar los trámites para los que tiene permisos, gracias a las políticas de uso previamente definidas.
- ✓ Si no existe un permiso establecido para un uso específico (por ejemplo, un trámite concreto), **Redtrust** le advertirá que se trata de un PERMISO DENEGADO. Ante esto, el administrador de **Redtrust** en la empresa comprobará en la consola de administración si está desactivado este permiso. En caso de que fuera así y tuviera que estar habilitado, el administrador concedería permiso al usuario para usar el certificado en dicho trámite o gestión.



**USUARIO:** Como usuario no es necesario tener ninguna formación: se trabaja desde el explorador y lo único que este percibe es que existe un control sobre esos certificados.

# Modalidades Redtrust

*¿Cómo adaptar Redtrust a las  
necesidades de tu empresa?*

# Modalidades **Redtrust**



**Redtrust** es un producto pensado para todas las empresas, disponible en las modalidades:



## **HSM**

Los certificados se almacenan y gestionan desde el servidor HSM, un sistema criptográfico basado en hardware ubicado en el cliente.



## **VIRTUAL**

La ubicación y disponibilidad del servicio es totalmente controlada por el cliente desde el servidor virtual *inhouse*.



## **CLOUD**

Los certificados digitales se almacenan y gestionan en la nube de Redtrust.







## **CLOUD MSP**

Versión híbrida entre Cloud y Virtual. Servidor virtual alojado en la nube de Redtrust.



# Modalidades Redtrust



	 HSM	 VIRTUAL	 CLOUD	 CLOUD MSP
Agente en máquinas cliente	✓	✓	✓	✓
Servidor en ubicación controlada por el cliente	✓	✓		
Ubicación y disponibilidad del servicio totalmente controlada por el cliente	✓	✓		
Servicio disponible en Internet			✓	✓
Licenciamiento por número de usuarios	✓	✓	✓	✓
Licenciamiento por número de certificados			✓	
Integración con AD o LDAP	✓	✓		
Integración con API Firma	✓	✓		✓
Posibilidad de más de 1 administrador	✓	✓		✓
Agentes (Windows / Linux)	✓	✓	✓	✓
Autenticación Single-Sign On mediante SAML	✓	✓	✓	✓
Facilidad de Despliegues	<b>Media - Alta</b>	<b>Media - Alta</b>	<b>Alta</b>	<b>Media - Alta</b>



# Algunos clientes de **Redtrust**

*Compañías del sector de la banca, seguros, salud, transporte, farmacia y Administración Pública, entre otros, ya depositan su confianza en Redtrust*



# Algunos clientes de Redtrust



**iGracias!**

