

Documento de Seguridad

ITM Platform



ITM Platform
PROJECTS ▪ PROGRAMS ▪ PORTFOLIO



www.itmplatform.com



@itmplatform

Índice

1.	Entornos SaaS y OnDemand	1
1.1.	Modos de configuración de ITM Platform	1
1.2.	Servidor	1
1.3.	Aplicación y base de datos	2
1.4.	Dominio	3
1.5.	Acceso	4
1.6.	Identificación de usuarios	4
2.	Acceso a ITM Platform	5
2.1.	Claves de acceso	5
2.2.	Licencias	6
2.3.	Roles	7
2.4.	Configuración de roles	8
2.5.	Asignación como jefe de proyecto, servicio o programa	10
2.6.	Company Admin	12
3.	Copia de seguridad	13
3.1.	Base de datos	13
3.2.	Ficheros Web	13
3.3.	Ubicación del servidor de Backup	13
3.4.	Encriptación y custodia	13
3.5.	Copia de seguridad al cliente y borrado de datos	14
3.6.	Espacio de las copias de seguridad	14
4.	Entorno de respaldo	15
5.	Control y actualizaciones de software	16
5.1.	Aplicación	16
5.2.	Sistema	16
6.	Seguridad de red	17
6.1.	Firewall y bloqueo de puertos	17
6.2.	Red de acceso y red de administración	17
6.3.	Bloqueo de redes sospechosas	17
7.	Control de seguridad y vulnerabilidades	18
7.1.	Control semanal	18
7.2.	Control mensual	18
7.3.	Control trimestral	18
8.	Disponibilidad y rendimiento	19

1. Entornos SaaS y OnDemand

ITM Platform ofrece diferentes configuraciones adaptándose a las necesidades de cada organización en seguridad, políticas y preferencias de cada cliente. Puede configurar desde entornos compartidos (**SaaS**) que no requieren ninguna adaptación, a entornos personalizados (**OnDemand**) para cada organización.

Generalmente, se recomienda el modelo de implantación de un entorno SaaS por ser más económico que los entornos OnDemand, donde todos los costes de la infraestructura se repercuten al cliente.

1.1. Modos de configuración de ITM Platform

ITM Platform ofrece por defecto el sistema SaaS (**Software como Servicio**) en una infraestructura compartida con todas las garantías y seguridad necesarias para garantizar la privacidad de la información de cada cliente.

Como ampliación del sistema SaaS, ITM Platform proporciona otros modos personalizados, desde el **SaaS dedicado** a diferentes configuraciones **OnDemand**, para cubrir las necesidades de cada cliente.

	Servidor			Aplicación y BBDD		Dominio		Acceso			Identificación	
	compartido	Servidor físico	Cloud	Compartida	Dedicada	app.itmplatform.com	Personalizado	Acceso http	Acceso https (ssl)	Acceso por VPN	Usuario/Clave de ITM	Usuario/Clave sincronizada
SaaS	✓			✓		✓		✓	✓		✓	
SaaS dedicado	✓				✓		✓	✓	✓		✓	
OnDemand Físico		✓			✓		✓	✓	✓		✓	
OnDemand Cloud			✓		✓		✓	✓	✓		✓	
OnDemand VPN			✓		✓		✓			✓	✓	
OnDemand VPN - Sync			✓		✓		✓			✓		(requiere estudio)

1.2. Servidor

Servidor compartido

En esta configuración por defecto de ITM Platform se comparte el entorno de ejecución entre los distintos clientes, garantizando en todo momento la seguridad de acceso a la información a través de la identificación de usuario. Sólo los usuarios de una organización tienen acceso a los datos de la misma y, a su vez, cada usuario accede a determinados contenidos según los permisos configurados en su perfil (rol).

En el modo Servidor compartido los recursos de máquina son compartidos por todos los clientes y, por lo tanto, el rendimiento de los recursos es el mismo para todos los clientes. ITM Platform garantiza el correcto dimensionamiento de los servidores y el rendimiento la aplicación.

El servidor compartido se utiliza tanto en la modalidad SaaS como en SaaS dedicado, donde se establece una instancia de la aplicación y la base de datos dentro del servidor compartido.

Servidor físico

Si el cliente lo requiere, ITM Platform permite configurar uno o varios servidores dedicados para la ejecución de su entorno. Los criterios de dimensionamiento de estos servidores físicos y su configuración son establecidos por el cliente pero administrados por ITM Platform como parte integrante de sus servidores.

La ampliación o modificación de la configuración de estos servidores dedicados requiere de intervenciones programadas más o menos complejas, que pueden demandar la suspensión temporal del servicio, por lo que no son recomendables en el caso de necesitar la máxima flexibilidad para su ampliación o modificación.

Servidor en Cloud

Este servicio está basado en sistemas Cloud de alta disponibilidad y permite configurar un servidor dedicado de forma flexible. A diferencia del servidor físico, este servidor virtual puede ser ampliado y configurado con gran facilidad y, por lo tanto, adaptarse a las necesidades del cliente en cada momento.

Adicionalmente, el servidor Cloud dedicado puede complementarse con servicios de VPN y/o integración del servidor en el sistema de identificación del cliente por medio de relaciones de confianza realizadas a través de la VPN.

Incluido en todas las modalidades

En todas las modalidades anteriores se incluyen (adaptados a cada entorno) los siguientes servicios:

- Administración del sistema
- Copia de seguridad
- Control y actualizaciones de software
- Chequeo de seguridad y vulnerabilidades
- Control de rendimiento y optimización del sistema

1.3. Aplicación y base de datos

Entorno compartido

En el entorno **SaaS** todos los clientes comparten la aplicación y la base datos de ITM Platform, optimizándose así la utilización de los recursos. ITM Platform garantiza en todo momento la seguridad de acceso a la información a través de la identificación de usuario. Sólo los usuarios de una organización tienen acceso a los datos de la misma y, a su vez, cada usuario accede a determinados contenidos según los permisos configurados en su perfil.

Entorno dedicado

Tanto en el entorno compartido (SaaS dedicado) como en los entornos OnDemand se puede configurar una instancia de ITM Platform completamente dedicada para un cliente, permitiendo así gestionar de forma independiente sus datos y sus usuarios.

En el entorno SaaS dedicado se comparte la máquina con otros clientes pero se dispone de una copia personalizada de la aplicación y se utiliza una instancia de base de datos completamente independiente. En este caso, los recursos de hardware y el sistema operativo se comparten, mientras que los datos y la aplicación están aislados de los otros clientes.

En los entornos OnDemand, tanto la máquina y el sistema como la aplicación y la base de datos son completamente independientes y utilizados por un único cliente, obteniendo así total independencia.

1.4. Dominio

app.itmplatform.com

Es el dominio predeterminado de ITM Platform y genérico para todos los clientes. Cada entorno y sus datos se diferencian a través de las claves de acceso. Este dominio es válido únicamente para el servicio SaaS.

Subdominio

En el caso de utilizar una configuración personalizada, bien desde el servicio SaaS dedicado o bien desde OnDemand, puede registrar un subdominio de itmplatform.com de la siguiente manera:

<nombre_empresa>.itmplatform.com

Este subdominio no tiene coste adicional para el cliente y se gestiona directamente por los servidores DNS de ITM Platform.

Dominio propio

ITM Platform ofrece a los clientes la posibilidad de registrar un dominio o subdominio de su dominio corporativo en caso de utilizar una configuración personalizada, bien desde el servicio SaaS dedicado o bien desde OnDemand.

Estos dominios o subdominios personalizados pueden registrarse de la manera que deseen, como por ejemplo itmplatform.<nombre_empresa>.com.

Los dominios propios son gestionados por el cliente y sus servidores DNS deben apuntar a las direcciones IP del servidor de ITM Platform.

1.5. Acceso

Protocolos HTTP y HTTPS

Los clientes pueden acceder al servidor donde está su entorno desde cualquier lugar con conexión a Internet a través de los protocolos HTTP y HTTPS (seguro). En caso de utilizar un dominio personalizado, el cliente deberá obtener un certificado de servidor para ese nombre de dominio si desea acceder con el protocolo HTTPS (seguro).

VPN

Aquellos clientes que deseen el acceso a ITM Platform sólo desde su red corporativa pueden solicitar la conexión al servidor por medio de una conexión VPN.

Este servicio de conexión por VPN sólo se presta actualmente con los servidores Cloud, si bien es posible estudiar esta solución para los servidores físicos.

1.6. Identificación de usuarios

Claves de acceso a ITM Platform

El acceso predeterminado a ITM Platform se realiza mediante las claves de usuario garantizando así el uso correcto y la seguridad de los datos .

Sincronización de la identificación

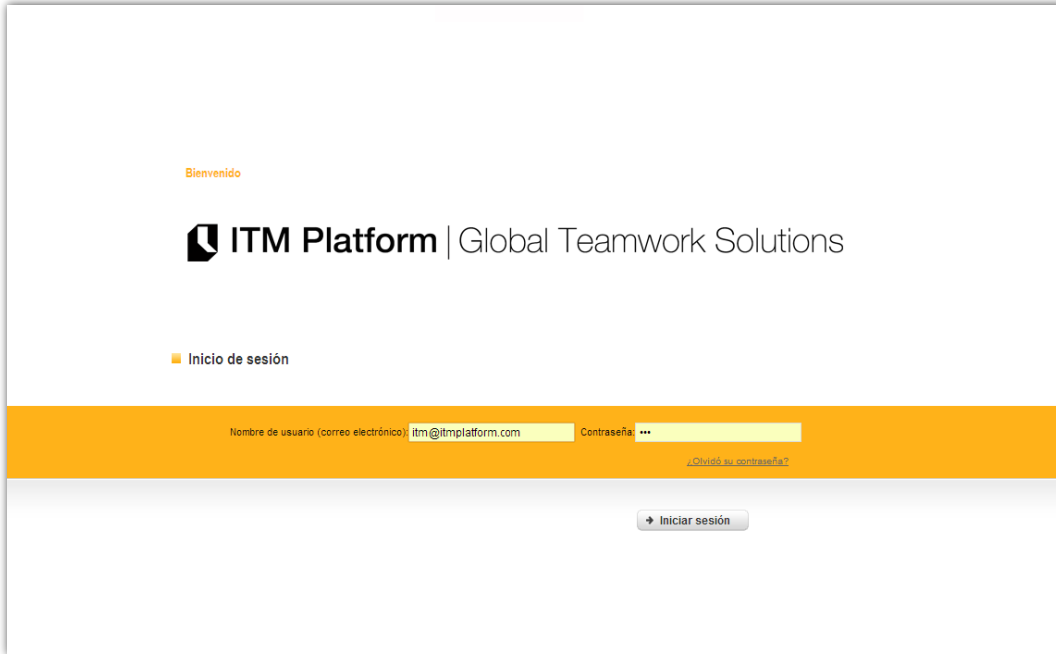
Si el cliente lo solicita, se pueden conectar los sistemas de identificación corporativos con los servidores de ITM Platform de forma que el acceso se realice con las claves utilizadas habitualmente por los usuarios de la organización.

Esta sincronización para la identificación de usuarios debe ser estudiada en cada caso, requiriendo para ello la conexión a través de VPN entre la red corporativa y los servidores de ITM Platform con el fin de garantizar la máxima seguridad.

2. Acceso a ITM Platform

2.1. Claves de acceso

ITM Platform permite el acceso al entorno a través de las claves de usuario.

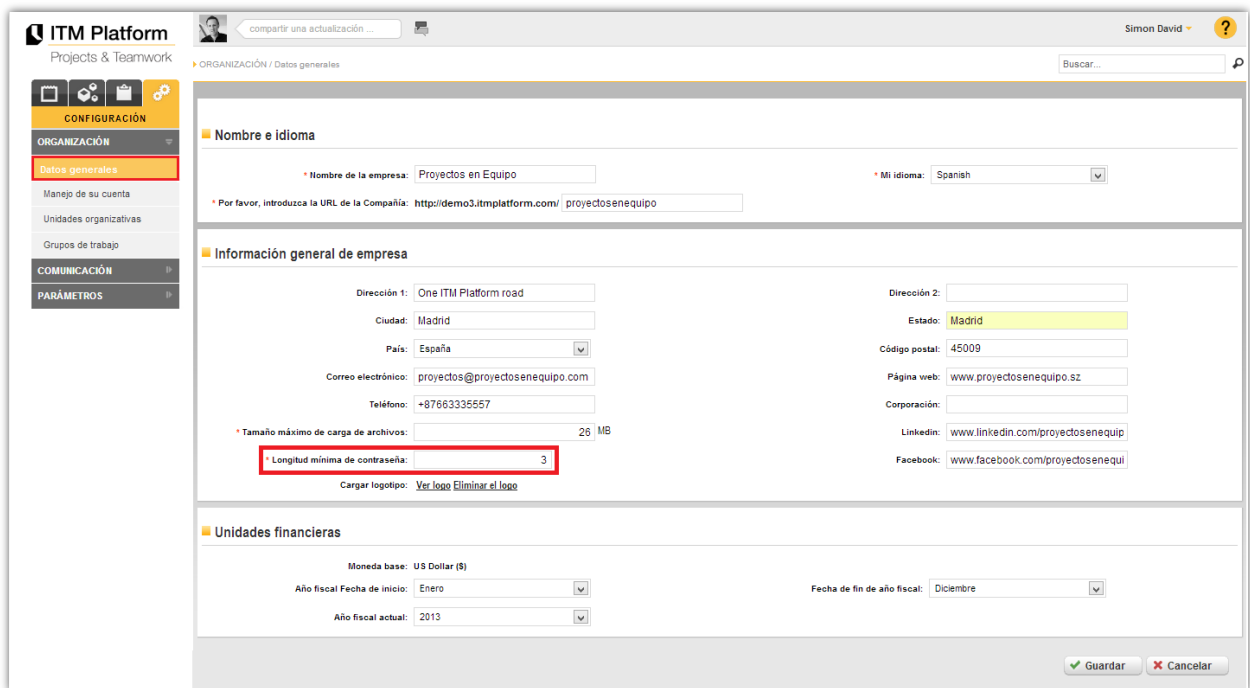


El nombre de usuario es la dirección de correo electrónico y donde recibirá las notificaciones del sistema. Cada usuario puede modificar su contraseña en cualquier momento:



Configuración de la longitud de la clave

Cada organización puede configurar de forma genérica la longitud de la contraseña con la que accede a su entorno. Este cambio sólo pueden realizarlo los usuarios cuyo rol les permita acceder a la ventana “Datos generales”.



The screenshot shows the 'Datos generales' configuration page in the ITM Platform. The page is divided into several sections:

- Nombre e idioma:** Nombre de la empresa: Projectos en Equipo; Mi idioma: Spanish.
- Información general de empresa:** Dirección 1: One ITM Platform road; Ciudad: Madrid; País: España; Correo electrónico: proyectos@proyectosenequipo.com; Teléfono: +87663335557; Dirección 2: (empty); Estado: Madrid; Código postal: 45009; Página web: www.proyectosenequipo.sz; Corporación: (empty); LinkedIn: www.linkedin.com/proyectosenequip; Facebook: www.facebook.com/proyectosenequi.
- Unidades financieras:** Moneda base: US Dollar (\$); Año fiscal Fecha de inicio: Enero; Año fiscal actual: 2013; Fecha de fin de año fiscal: Diciembre.

A red box highlights the 'Longitud mínima de contraseña' field, which is set to 3.

Recuperación de contraseña

Si un usuario olvida o pierde su contraseña puede solicitarla de nuevo a través de la opción “¿Olvidó su contraseña?” y recibirá un correo electrónico con las claves en la dirección de correo utilizada como nombre de usuario.

2.2. Licencias

Cuando un cliente adquiere una solución de ITM Platform obtiene el derecho de uso de unas licencias que le permiten acceder a las diferentes funcionalidades de ITM Platform.

Las licencias configuran las funciones adquiridas por un cliente en un entorno personalizado. Un cliente puede tener licencias de cada una de las soluciones de ITM Platform, de manera que cada licencia determinará el acceso a unas funcionalidades u otras.

Las licencias, cuyo coste y condiciones varían, definen a su vez dos aspectos relevantes para el acceso a las funcionalidades:

Acceso a funciones

Estas funciones permiten asignar al usuario como:

- Jefe de Proyecto
- Gestor del Servicio
- Gerente del Programa

Si la licencia no dispone de este tipo de funciones, no podrá asignar ninguno de los roles anteriores.

Vea el capítulo Asignación como jefe de proyecto, servicio o programa para más información.

Acceso a funcionalidades

Las licencias configuran el acceso de cada usuario a determinadas funcionalidades del entorno. En cada licencia a su vez se puede configurar los roles de usuario que permiten una mayor o menor conjunto de funciones a las que puede acceder. Vea el capítulo 2.3 *Roles* para más información.

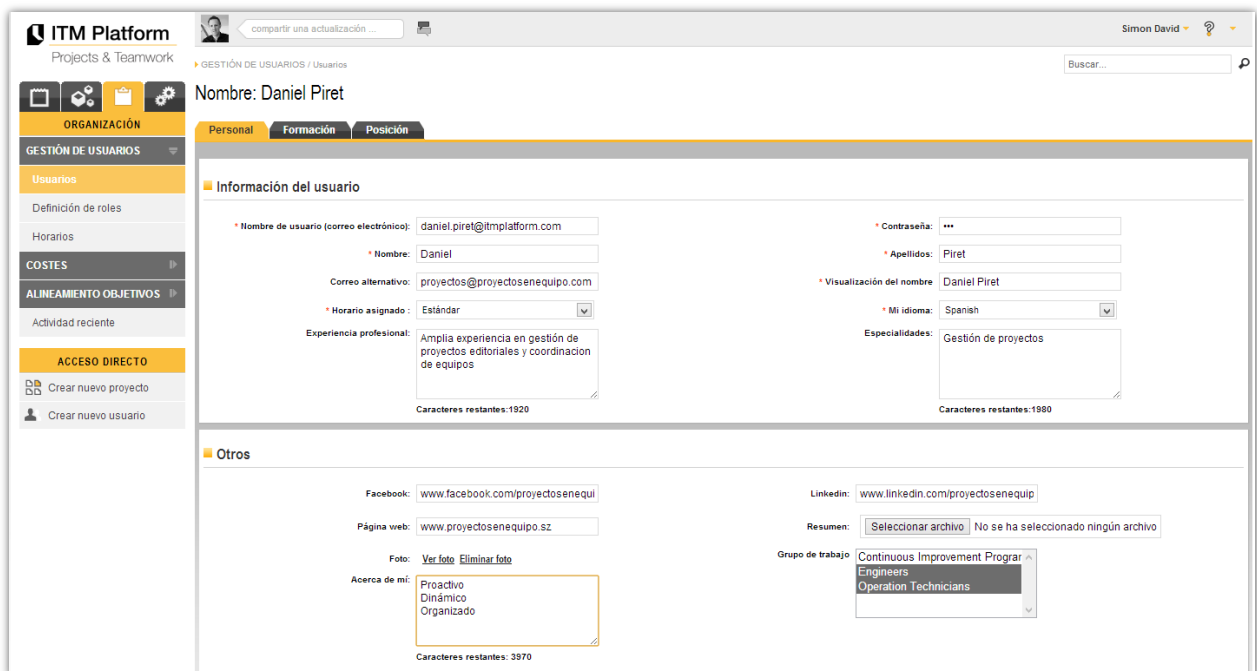
Procedimiento de actualización

La actualización del sistema de licencias se realiza desde el departamento de desarrollo de producto.

2.3. Roles

Asignación a usuarios

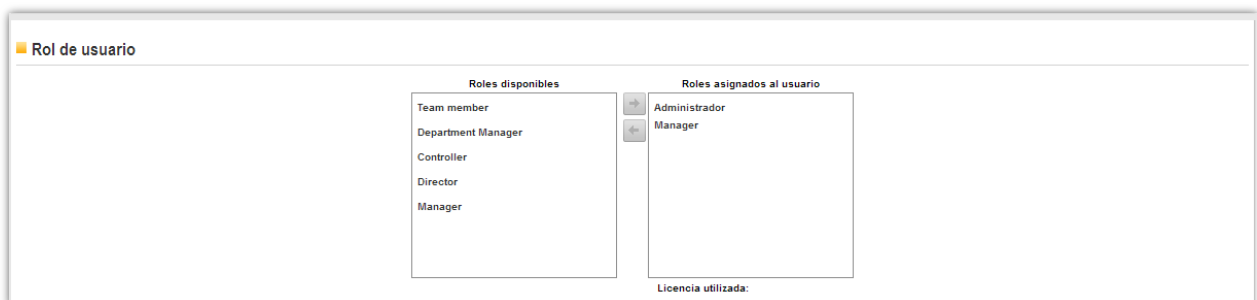
Cuando se crea un usuario debe tener asignado un rol. Por defecto, ITM Platform asigna un rol a cada usuario creado.



The screenshot shows the 'Gestión de Usuarios' interface for user 'Daniel Piret'. The interface is divided into several sections:

- Personal:**
 - Nombre de usuario (correo electrónico): daniel.piret@itmplatform.com
 - Nombre: Daniel
 - Apellido: Piret
 - Visualización del nombre: Daniel Piret
 - Contraseña: [oculto]
 - Correo alternativo: proyectos@proyectosenequipo.com
 - Mi idioma: Spanish
 - Horario asignado: Estándar
 - Experiencia profesional: Amplia experiencia en gestión de proyectos editoriales y coordinación de equipos (Caracteres restantes: 1920)
 - Especialidades: Gestión de proyectos (Caracteres restantes: 1980)
- Otros:**
 - Facebook: www.facebook.com/proyectosenequi
 - LinkedIn: www.linkedin.com/proyectosenequip
 - Página web: www.proyectosenequipo.sz
 - Resumen: [Seleccionar archivo] No se ha seleccionado ningún archivo
 - Foto: [Ver foto] [Eliminar foto]
 - Grupo de trabajo: Continuous Improvement Program, Engineers, Operation Technicians
 - Acerca de mí: Proactivo, Dinámico, Organizado (Caracteres restantes: 3570)

Un usuario puede tener más de un rol asignado, y en este caso, los permisos de ambos roles se suman, es decir, tendrá todas las funciones disponibles en cada rol.



The 'Rol de usuario' interface shows two columns of roles:

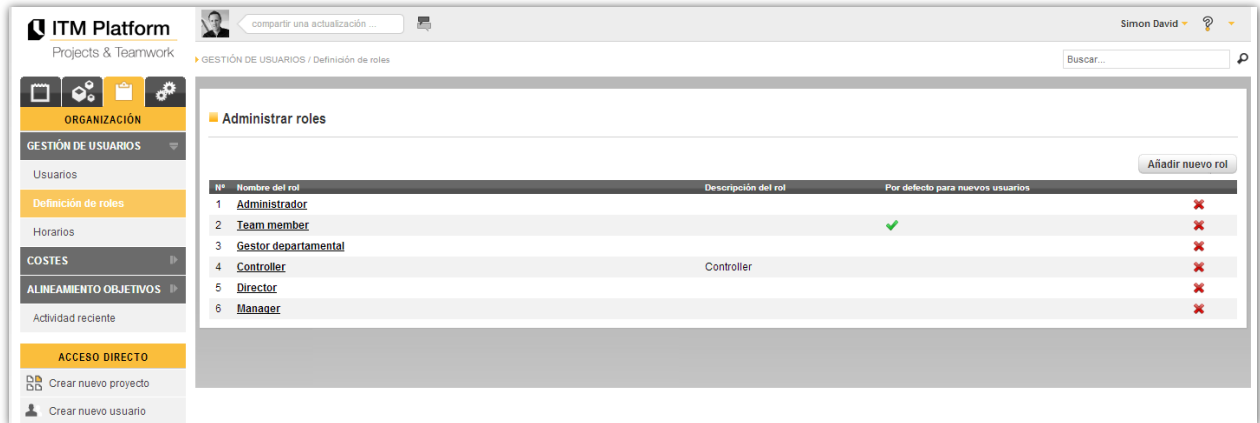
- Roles disponibles:** Team member, Department Manager, Controller, Director, Manager.
- Roles asignados al usuario:** Administrador, Manager.

Below the columns, it indicates 'Licencia utilizada:'.

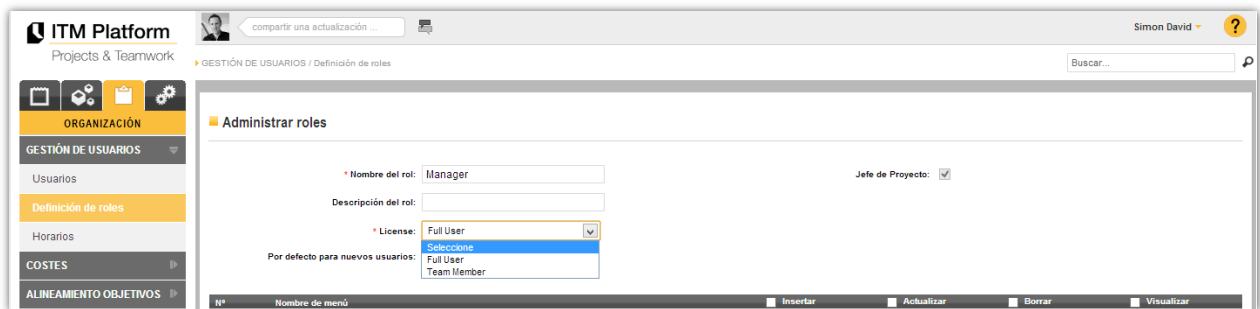
La funcionalidad para crear usuarios y asignar roles solo está disponible para usuarios cuyo rol permita acceder a la opción "Usuarios".

2.4. Configuración de roles

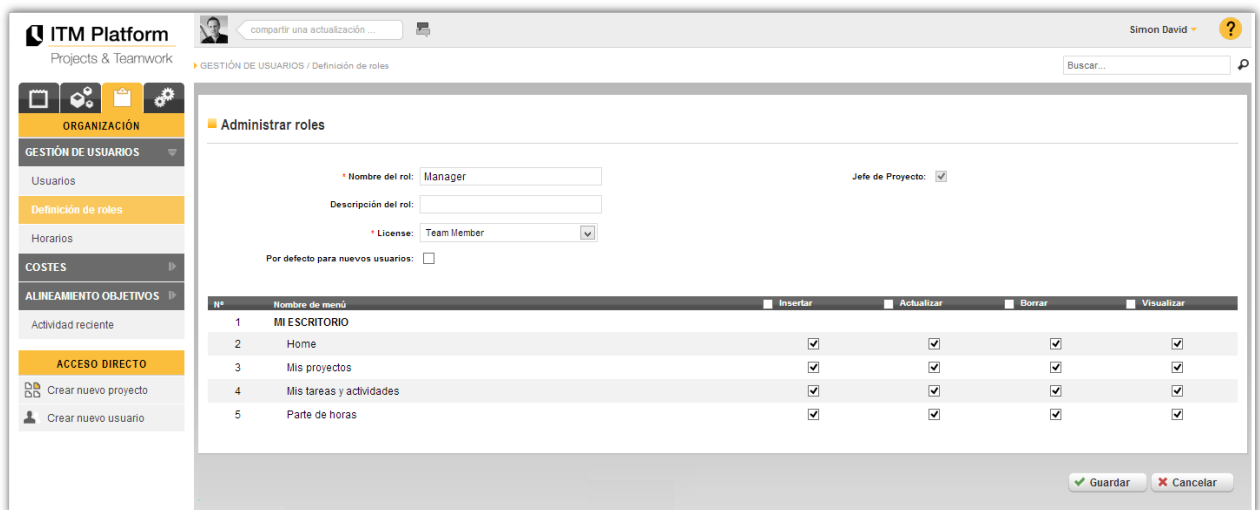
ITM Platform ofrece varios roles preconfigurados pero puede modificar, añadir o eliminar cuantos roles considere necesarios:



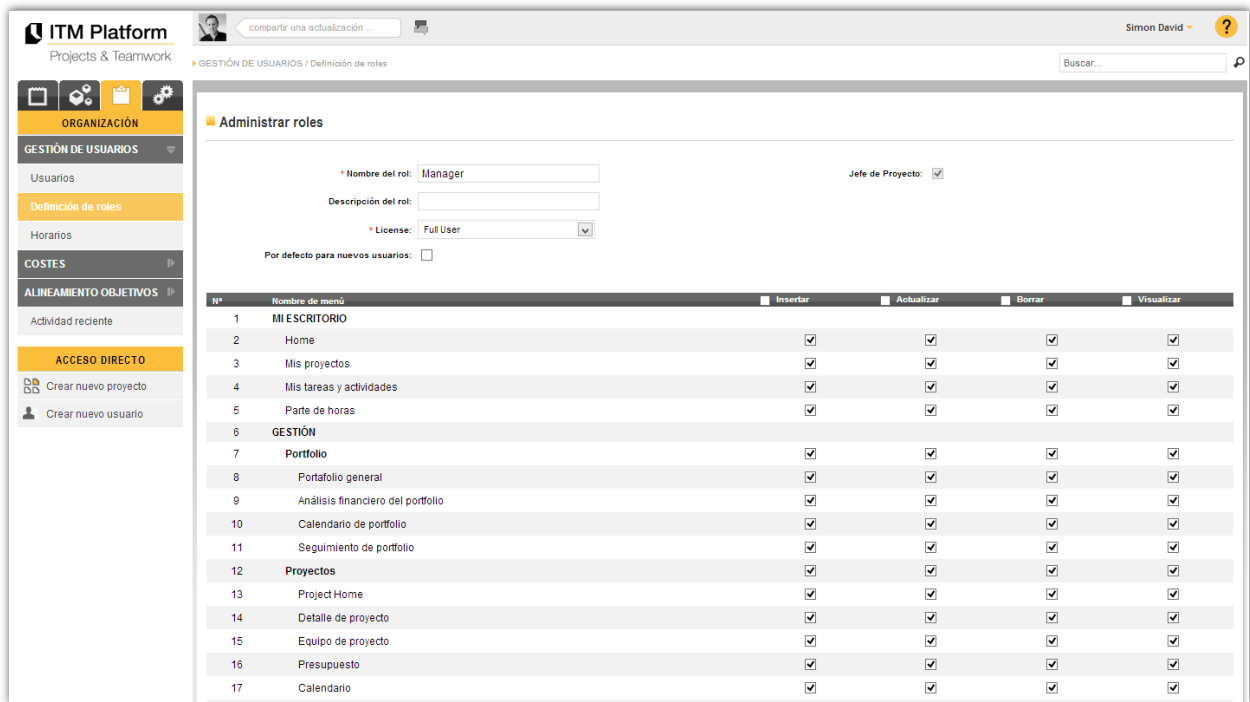
Un paso fundamental en la creación de un nuevo rol es la asignación de la licencia que va a utilizar ese rol y, por lo tanto, la configuración básica de *Acceso a funciones* y *Acceso a funcionalidades*:



Puede configurar algunas opciones del rol **Team Member** pero no permite asignarlo como jefe de proyecto, servicio o programa:



El rol **Full Access** permite configurar todas las opciones de este rol y asignar al usuario como jefe de proyecto, servicio o programa:



Administrar roles

Nombre del rol: Jefe de Proyecto:

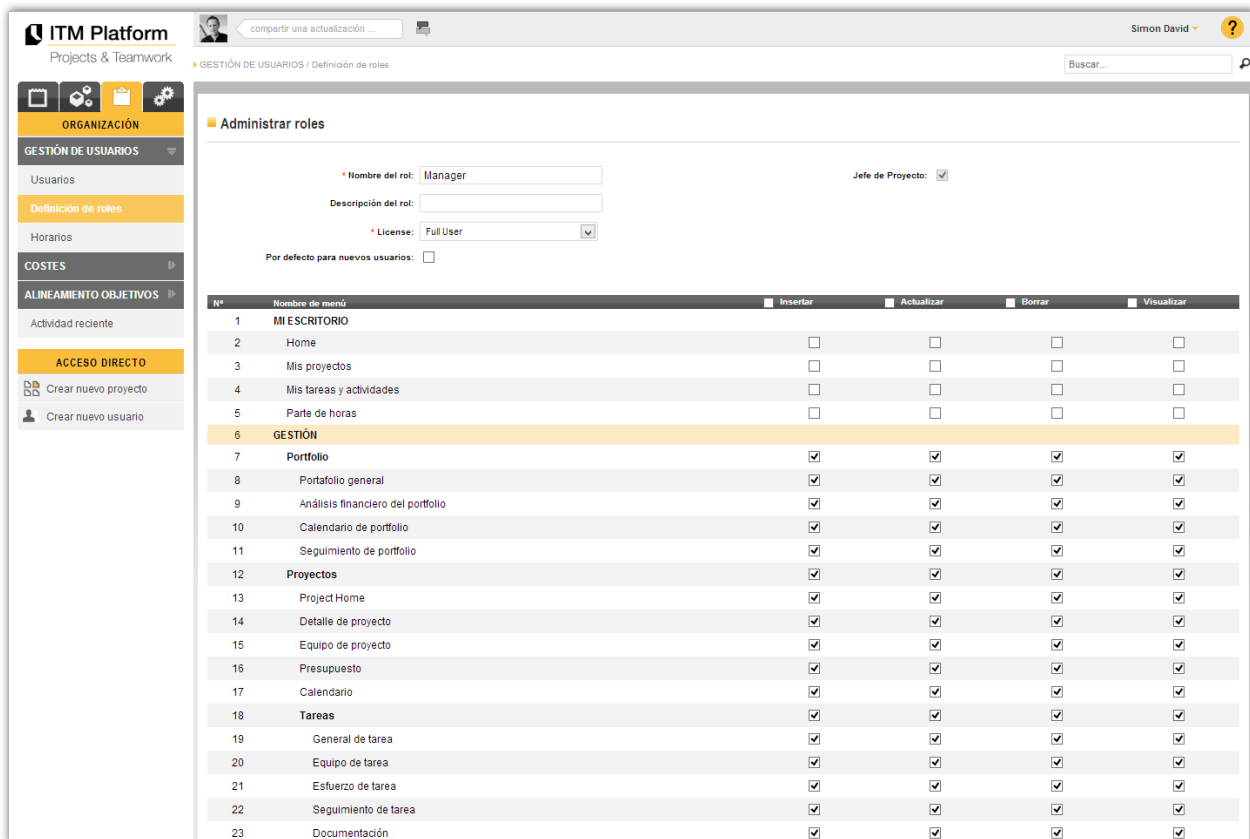
Descripción del rol:

License:

Por defecto para nuevos usuarios:

Nº	Nombre de menú	Insertar	Actualizar	Borrar	Visualizar
1	MI ESCRITORIO				
2	Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Mis proyectos	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Mis tareas y actividades	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Parte de horas	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	GESTIÓN				
7	Portfolio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Portafolio general	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Análisis financiero del portfollio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Calendario de portfollio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Seguimiento de portfollio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Proyectos	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Project Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Detalle de proyecto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Equipo de proyecto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Presupuesto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Calendario	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

En este ejemplo se configura un rol con acceso a todas las opciones de la función **GESTIÓN**:



Administrar roles

Nombre del rol: Jefe de Proyecto:

Descripción del rol:

License:

Por defecto para nuevos usuarios:

Nº	Nombre de menú	Insertar	Actualizar	Borrar	Visualizar
1	MI ESCRITORIO				
2	Home	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Mis proyectos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Mis tareas y actividades	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Parte de horas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	GESTIÓN				
7	Portfolio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Portafolio general	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Análisis financiero del portfollio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Calendario de portfollio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Seguimiento de portfollio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Proyectos	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Project Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Detalle de proyecto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Equipo de proyecto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Presupuesto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Calendario	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Tareas	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	General de tarea	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Equipo de tarea	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Esfuerzo de tarea	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Seguimiento de tarea	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Documentación	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

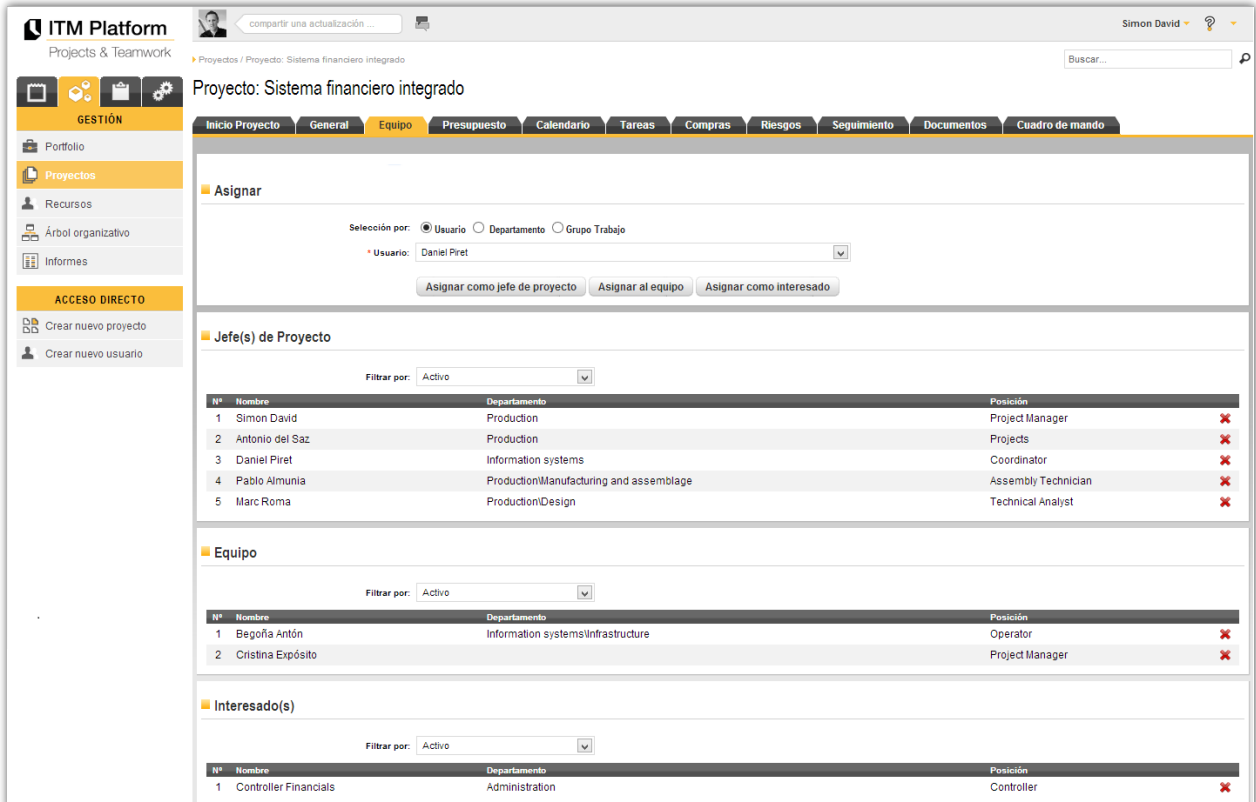
Como resultado el usuario verá esta configuración de menú:



La funcionalidad para crear usuarios y asignar roles sólo está disponible para usuarios cuyo rol permita acceder a la opción “Definición de roles”.

2.5. Asignación como jefe de proyecto, servicio o programa

Cuando asigna un usuario de ITM Platform en el equipo de un proyecto, servicio o programa, puede configurarlo como usuario interesado (project guest), miembro del equipo (team member) o jefe (manager).



Asignar

Selección por: Usuario Departamento Grupo Trabajo

* Usuario: Daniel Piret

Asignar como jefe de proyecto Asignar al equipo Asignar como interesado

Jefe(s) de Proyecto

Filtrar por: Activo

N°	Nombre	Departamento	Posición
1	Simon David	Production	Project Manager
2	Antonio del Saz	Production	Projects
3	Daniel Piret	Information systems	Coordinator
4	Pablo Almunia	Production/Manufacturing and assemblage	Assembly Technician
5	Marc Roma	Production/Design	Technical Analyst

Equipo

Filtrar por: Activo

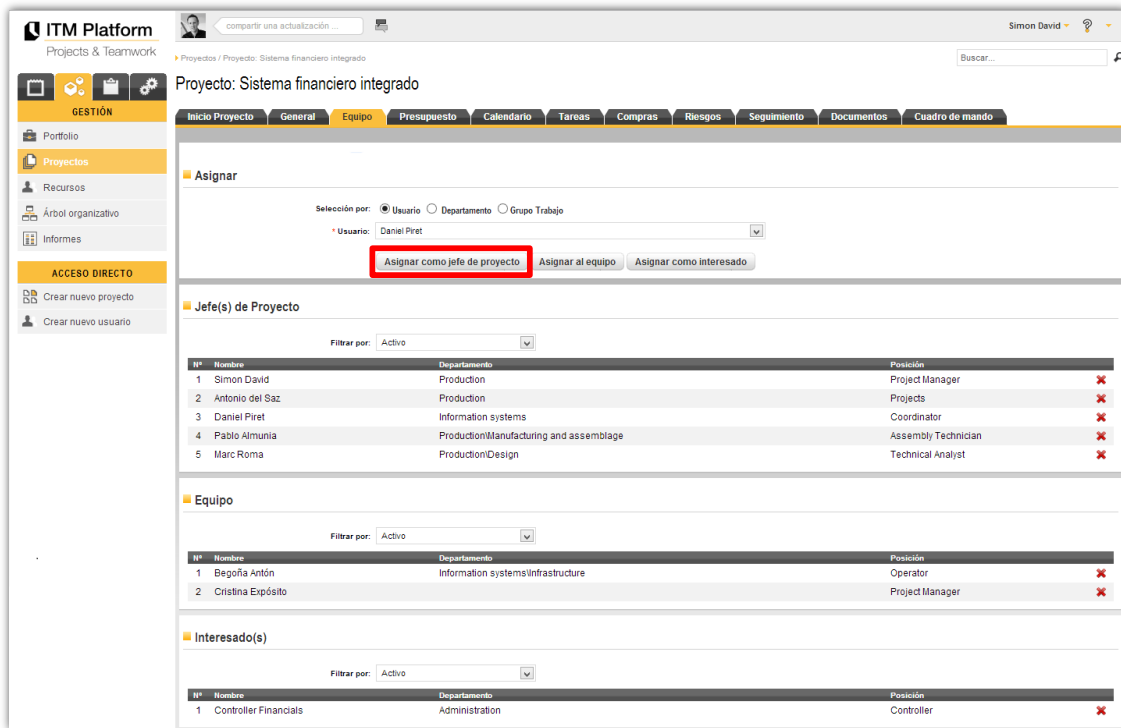
N°	Nombre	Departamento	Posición
1	Begoña Antón	Information systems/Infrastructure	Operator
2	Cristina Expósito		Project Manager

Interesado(s)

Filtrar por: Activo

N°	Nombre	Departamento	Posición
1	Controller Financials	Administration	Controller

Al asignar un usuario como jefe de proyecto, servicio o programa, ITM Platform comprueba que el usuario tiene un rol que permite esta asignación.



ITM Platform Projects & Teamwork

Proyectos / Proyecto: Sistema financiero integrado

Proyecto: Sistema financiero integrado

Asignar

Selección por: Usuario Departamento Grupo Trabajo

Usuario: Daniel Piret

Asignar como jefe de proyecto | Asignar al equipo | Asignar como interesado

Jefe(s) de Proyecto

Filtrar por: Activo

ID	Nombre	Departamento	Posición
1	Simon David	Production	Project Manager
2	Antonio del Saz	Production	Projects
3	Daniel Piret	Information systems	Coordinator
4	Pablo Almunia	Production/Manufacturing and assemblage	Assembly Technician
5	Marc Roma	Production/Design	Technical Analyst

Equipo

Filtrar por: Activo

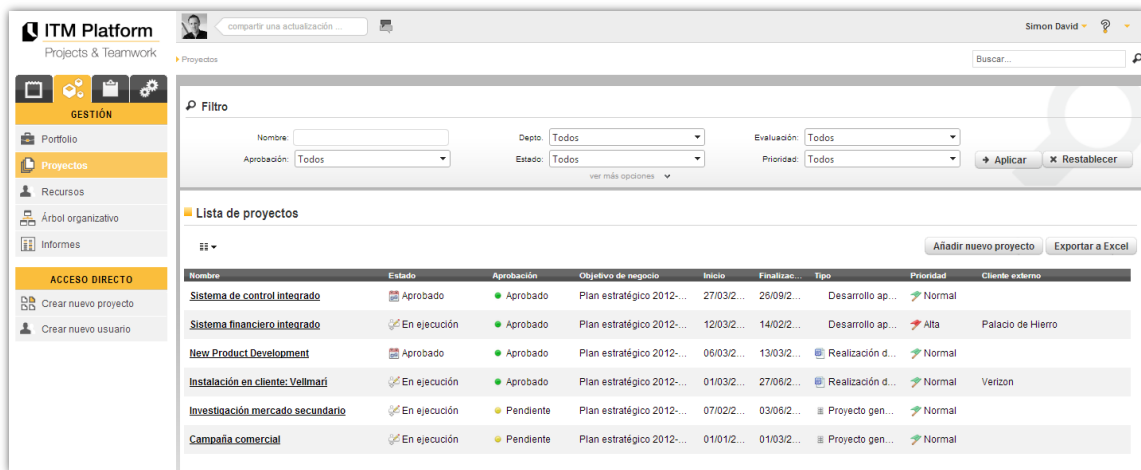
ID	Nombre	Departamento	Posición
1	Begoña Antón	Information systems/Infrastructure	Operator
2	Cristina Expósito		Project Manager

Interesado(s)

Filtrar por: Activo

ID	Nombre	Departamento	Posición
1	Controller Financials	Administration	Controller

Cuando un usuario es asignado como interesado (project guest), miembro de equipo (team member) o jefe (manager) en un proyecto o servicio, puede acceder a las opciones “Mis proyectos” o “Mis servicios”. Esto no ocurre así con los Programas, que sólo están disponibles desde la pestaña GESTIÓN.



ITM Platform Projects & Teamwork

Proyectos

Filtro

Nombre: [] Depto: Todos Evaluación: Todos

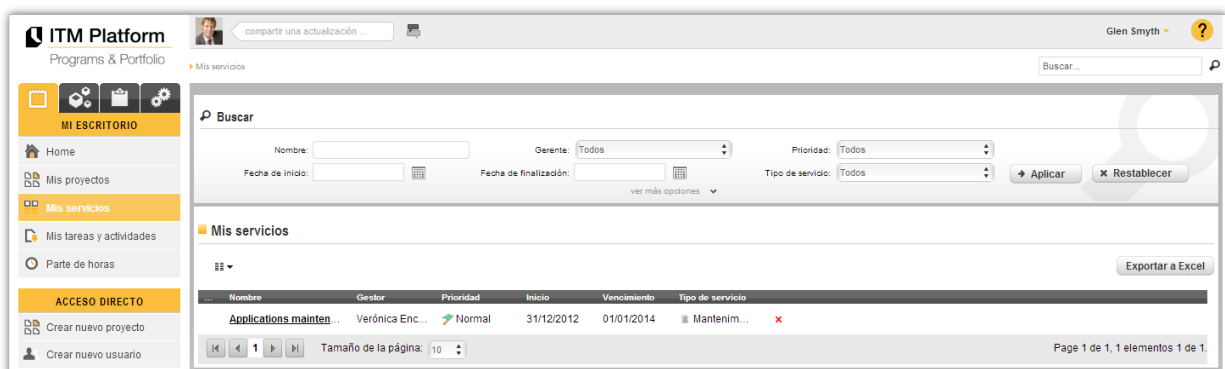
Aprobación: Todos Estado: Todos Prioridad: Todos

Aplicar | Restablecer

Lista de proyectos

Añadir nuevo proyecto | Exportar a Excel

Nombre	Estado	Aprobación	Objetivo de negocio	Inicio	Finalizac...	Tipo	Prioridad	Cliente externo
Sistema de control integrado	Aprobado	Aprobado	Plan estratégico 2012-...	27/03/2...	26/09/2...	Desarrollo ap...	Normal	
Sistema financiero integrado	En ejecución	Aprobado	Plan estratégico 2012-...	12/03/2...	14/02/2...	Desarrollo ap...	Alta	Palacio de Hierro
New Product Development	Aprobado	Aprobado	Plan estratégico 2012-...	08/03/2...	13/03/2...	Realización d...	Normal	
Instalación en cliente: Vellmari	En ejecución	Aprobado	Plan estratégico 2012-...	01/03/2...	27/06/2...	Realización d...	Normal	Verizon
Investigación mercado secundario	En ejecución	Pendiente	Plan estratégico 2012-...	07/02/2...	03/06/2...	Proyecto gen...	Normal	
Campaña comercial	En ejecución	Pendiente	Plan estratégico 2012-...	01/01/2...	01/03/2...	Proyecto gen...	Normal	



ITM Platform Programs & Portfolio

Mis servicios

Buscar

Nombre: [] Cliente: Todos Prioridad: Todos

Fecha de inicio: [] Fecha de finalización: [] Tipo de servicio: Todos

Aplicar | Restablecer

Mis servicios

Exportar a Excel

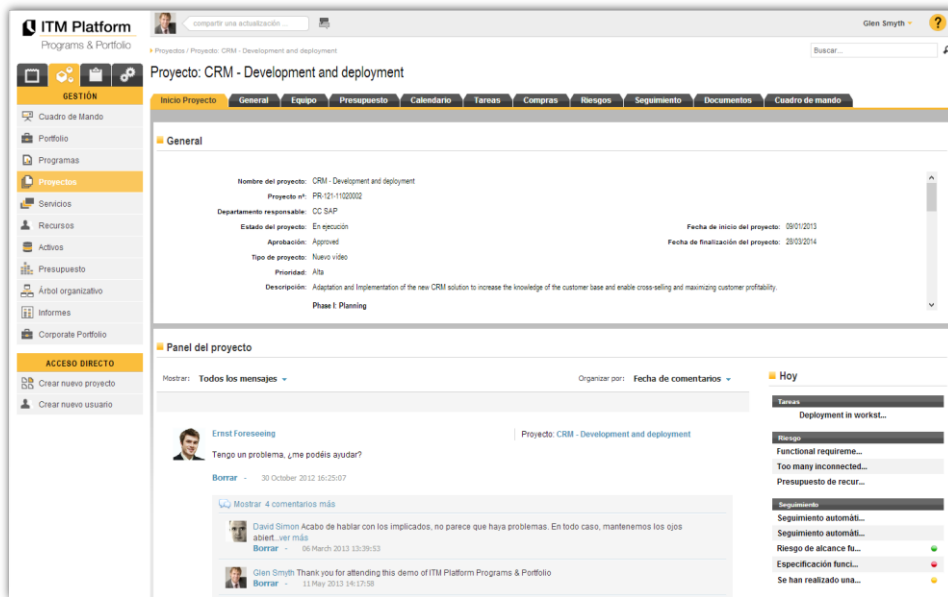
Nombre	Gestor	Prioridad	Inicio	Vencimiento	Tipo de servicio
Applications mainten...	Verónica Enc...	Normal	31/12/2012	01/01/2014	Mantenim...

Tamaño de la página: 10

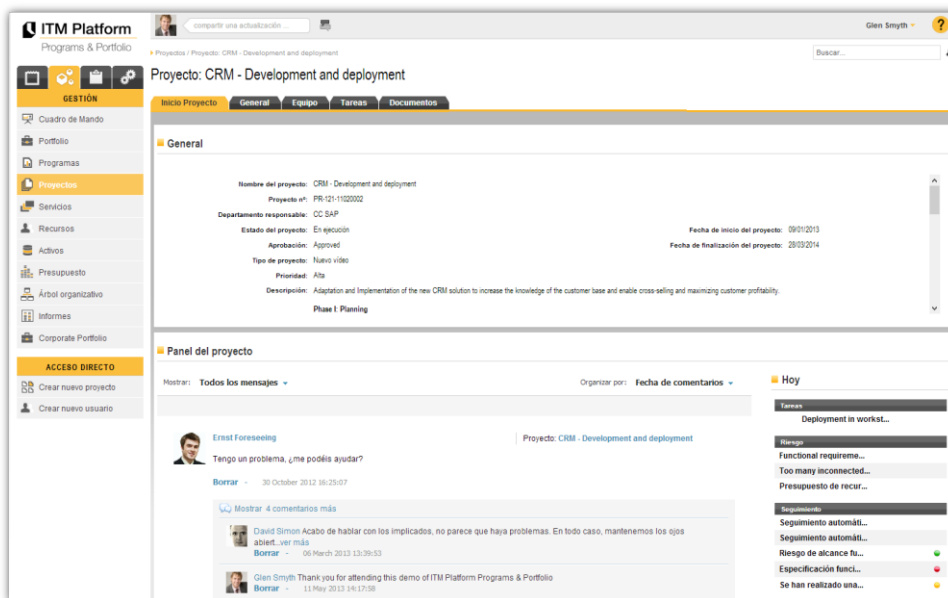
Page 1 de 1, 1 elementos 1 de 1

Cuando se accede a un proyecto o servicio desde el menú “Mis proyectos” o “Mis servicios” respectivamente, puede disponer de dos opciones, dependiendo si el usuario es jefe (manager) o miembro de equipo (team member).

Si el usuario ha sido asignado como jefe, dispondrá de permisos de lectura y escritura.



Si el usuario ha sido asignado como miembro de equipo, sólo tiene permiso de lectura.



2.6. Company Admin

ITM Platform ofrece, además de los usuarios mencionados anteriormente, el usuario “Company Admin”. Este usuario es quién crea el entorno y tiene acceso completo a todas las funcionalidades sin ninguna restricción por tipo de licencias o roles.

3. Copia de seguridad

3.1. Base de datos

ITM Platform realiza de forma automática una copia de la base de datos cada dos horas. Una vez realizada la copia, se comprime y se cifra, y a continuación, la versión abierta se elimina y la cifrada se envía al servidor de backup. Posteriormente, se almacena en el servidor de producción donde se ha realizado y finalmente se envía un correo electrónico a los operadores para el control de copias.

Transcurridos siete días del almacenamiento de la copia en el servidor de producción, se elimina pero se mantiene en el servidor de backup.

El mantenimiento de las copias de seguridad en el servidor de producción tiene como único objetivo garantizar la máxima rapidez de recuperación de datos ante una incidencia de nivel medio.

3.2. Ficheros Web

Los ficheros de la web, incluidos los documentos que son subidos por los usuarios, son copiados una vez al día comprimidos y cifrados en el servidor de producción y el servidor de backup.

Al mes son eliminados del servidor de producción pero se mantiene una copia de seguridad semanal en el servidor de backup durante un año.

3.3. Ubicación del servidor de Backup

El servidor de backup está ubicado en las instalaciones de un proveedor externo y por lo tanto no están sujetas a la disponibilidad y acceso a nuestros servidores de producción.

3.4. Encriptación y custodia

Todas las copias de seguridad están cifradas con algoritmos fuertes y claves de 64 bits para protegerlas de operaciones indebidas.

Las copias de seguridad sólo residen en los servidores de producción y el servidor de backup. Los servidores de respaldo no disponen de datos hasta que no son convertidos en servidores de producción con el fin de evitar posibles descuidos en su seguridad.

Cualquier procedimiento con las copias de seguridad se anota en el libro de operaciones y sólo el equipo de operaciones puede manipular las copias.

3.5. Copia de seguridad al cliente y borrado de datos

En el caso de que un cliente solicite una copia de seguridad de sus datos, el equipo de atención al cliente comprobará primero si la persona que lo solicita está autorizada a disponer de los datos para su recuperación.

El equipo de operaciones sólo atenderá aquellas solicitudes de copia de seguridad autorizadas por el departamento de atención al cliente y no responderá a peticiones directas del departamento de soporte.

Si un cliente solicita el borrado completo de alguna o toda la información de la base de datos, ésta se eliminará de la misma y se creará una copia de seguridad adicional con los datos eliminados.

Esta copia de seguridad adicional se marcará como Snapshot especial ya que no se podrán realizar restauraciones de datos con copias de seguridad anteriores a este snapshot. No existen mecanismos para borrar datos de clientes de copias de seguridad ya realizadas.

3.6. Espacio de las copias de seguridad

Estos son algunos datos aproximados de ocupación de las copias de seguridad:

Plan de copias de seguridad

Base de Datos			
Debe realizarse copias de seguridad bastantes veces para asegurar que podemos recuperar los datos de los clientes con una mínima pérdida de datos.			
Fechas	Copia	nº	Ubicación
Entre ahora y 7 días	Copia de seguridad cada 2 horas	84	Servidor principal y servidor backup
Entre 7 días y 1 mes	Copia de seguridad primera de cada día	25	Servidor principal y servidor backup
Entre 1 mes y 12 meses	Copia de seguridad primera de cada lunes	48	Servidor de backup
		nº	espacio ocupado
Copias de 12 meses		241	24.100 MB
Servidor principal		84	8.400 MB
Servidor de backup		157	15.700 MB
Tamaño medio comprimido			100 MB

Web			
Se pueden hacer menos copias de seguridad. Es conveniente tener varias versiones para poder volver a una versión anterior en caso de detectar una actualización desastrosa, pero no es necesario gestionar muchas copias.			
Fechas	Copia	nº	Ubicación
Entre ahora y 1 mes	Copia diaria a las 01:00 UTC	31	Servidor principal y servidor backup
Entre 1 mes y 12 meses	Copia de seguridad primera de cada lunes	48	Servidor de backup
		nº	espacio ocupado
Copias de 12 meses		110	5.500 MB
Servidor principal		31	1.550 MB
Servidor de backup		79	3.950 MB
Tamaño medio comprimido			50 MB

4. Entorno de respaldo

Existe un entorno de respaldo preparado para recuperar el sistema en caso de incidencia grave que impida a los servidores de producción dar servicio.

Este entorno de respaldo se encuentra en un proveedor de servicio externo y por lo tanto no está sujeto a la disponibilidad y acceso a nuestros servidores de producción.

En caso de incidencia grave en los servidores de producción, se ejecutará el plan de contingencia que en líneas generales establece los siguientes protocolos:

- Bloqueo completo del acceso a los servidores de producción dando un aviso de incidencia y, de esta forma, evitar que algunos clientes continúen accediendo a los servidores en una situación de caída
- Comprobación del nivel de versión del software en los servidores alternativos y actualización, si fuera necesario, de la copia de seguridad desde del servidor de backup
- Obtención de la copia de seguridad de la base de datos del servidor de backup y restauración en los servidores de respaldo
- Comprobación general del sistema
- Redirección del acceso de los clientes al servidor de respaldo

Una vez solventada la incidencia se ejecuta el procedimiento de recuperación del entorno de producción a partir de las copias de seguridad del entorno de respaldo y, siempre, dentro de una intervención planificada con antelación y comunicada a los usuarios.

Una vez al año se realizará un simulacro de incidencia para comprobar que todos los procedimientos están actualizados y son correctos, y que sea posible activar los servidores de respaldo en menos de dos horas desde la caída del sistema.

5. Control y actualizaciones de software

5.1. Aplicación

Entornos

ITM Platform dispone de dos entornos previos a la puesta en producción de cualquier actualización :

- **Test:** primer nivel de confirmación del software donde se comprueba que cada actualización es:
 - o Completa: revisión de que ficheros, componentes y otros elementos están presentes.
 - o Correcta: se comprueba que las modificaciones o nuevas funcionalidades son correctas y ejecutan sus operaciones acorde a las especificaciones funcionales.
 - o Respetuosa: se realizan pruebas para comprobar que otras funcionalidades, en principio no afectadas, mantienen sus especificaciones funcionales.
 - o Segura: se realiza una batería de pruebas de seguridad que incluye inyección de código, control de acceso y ataques de denegación de servicio.
 - o Eficiente: se realiza una monitorización del sistema para comprobar que mantiene el mismo rendimiento y no hay bloqueos u otras incidencias de ejecución que puedan afectar a la plataforma.
- **Demo:** en este entorno se repiten las pruebas del entorno Test y se realiza una segunda fase de pruebas, especialmente aquellas que tienen que ver con datos, ya que este entorno incluye datos de organizaciones que son actualizados regularmente. Además se verifica que cada actualización es:
 - o Integra: se revisan los datos existentes antes de la actualización y se comprueba que los valores siguen siendo los mismos o equivalentes si se han producido modificaciones que afectan a los datos.
 - o Consistente: se revisa que los datos existentes y los nuevos se comportan de la forma esperada y no se producen inconsistencias entre las distintas entidades.
- **App:** entorno de producción donde, una vez superadas todas las pruebas, se actualiza ITM Platform.

Autorización y comunicación

Es necesaria la aprobación del equipo funcional, el de sistemas y el de seguridad para proceder a la actualización del entorno de producción. Si alguno de estos equipos no estuviera de acuerdo volvería al equipo de desarrollo. Una vez aprobada la actualización se comunica la fecha de puesta en producción al equipo de operaciones y de soporte.

5.2. Sistema

El software de los servidores se actualiza exclusivamente por el equipo de operaciones. El mantenimiento durante el fin de semana incluye revisión de actualizaciones, parches y soluciones de los fabricantes de los sistemas operativos y software base de todos los servidores de ITM Platform.

En el caso de que algún fabricante comunique un aviso de actualización urgente, el equipo de sistemas de ITM Platform evaluará las ventajas o riesgos de realizar esta actualización fuera de los mantenimientos programados.

6. Seguridad de red

6.1. Firewall y bloqueo de puertos

ITM Platform dispone de un primer nivel de acceso por medio de un firewall externo que filtra todos los intentos de acceso a puertos y direcciones de los servidores.

Dicho firewall tiene una sonda que advierte de ataques de denegación de servicio y accesos sospechosos que puedan poner en riesgo la seguridad.

Todos los servidores disponen de filtros adicionales de seguridad donde se bloquean todos los puertos y direcciones que no son estrictamente necesarios. Si se intenta realizar un acceso a un puerto o dirección bloqueados se emite un aviso de seguridad.

6.2. Red de acceso y red de administración

Todos los servidores disponen de dos tarjetas de red, una conectada a la red de administración y otra conectada a la red de acceso general.

El acceso a la red de administración sólo está disponible para el personal de operaciones que accede a las consolas de administración de los distintos servidores. Esta red tiene un tráfico muy restringido y permite el acceso a los servidores en caso de ataques de denegación de servicio por llamadas masivas a los servidores.

La red de acceso general se utiliza para acceder por medio de protocolos HTTP y HTTPS a los servidores web públicos. Esta red sólo permite accesos a los puertos y dominios adecuados, pero también se controla especialmente cualquier vulnerabilidad que pueda existir.

6.3. Bloqueo de redes sospechosas

Si durante los procedimientos de revisión hay intentos de acceso desde redes sospechosas, se establece un protocolo de seguridad adicional que bloquea estas redes con el fin de evitar ataques de servidores zombi u otro tipo de ataque masivo desde ubicaciones no controladas.

7. Control de seguridad y vulnerabilidades

7.1. Control semanal

En los procedimientos de operación estándar semanales se realiza:

- Comprobación de las actualizaciones de los sistemas operativos y software base
- Ejecución completa de los antivirus de los servidores
- Escaneo general de los servidores con el fin de detectar cualquier cambio en la configuración del firewall, acceso de puertos o direcciones no autorizados, o bien cualquier otra brecha en la seguridad de la red
- Lectura de los log de acceso denegado para identificar intentos de accesos no autorizados

7.2. Control mensual

En los procedimientos estándar el primer fin de semana de cada mes se realiza:

- Una revisión general del software de los servidores, comprobando la configuración del sistema y la versión de todos los ficheros clave
- Ejecución de una batería extendida de controles de seguridad

7.3. Control trimestral

Cada trimestre una empresa externa realiza una evaluación de seguridad y simula diferentes ataques contra la instalaciones para comprobar que no existe ninguna vulnerabilidad en la seguridad.

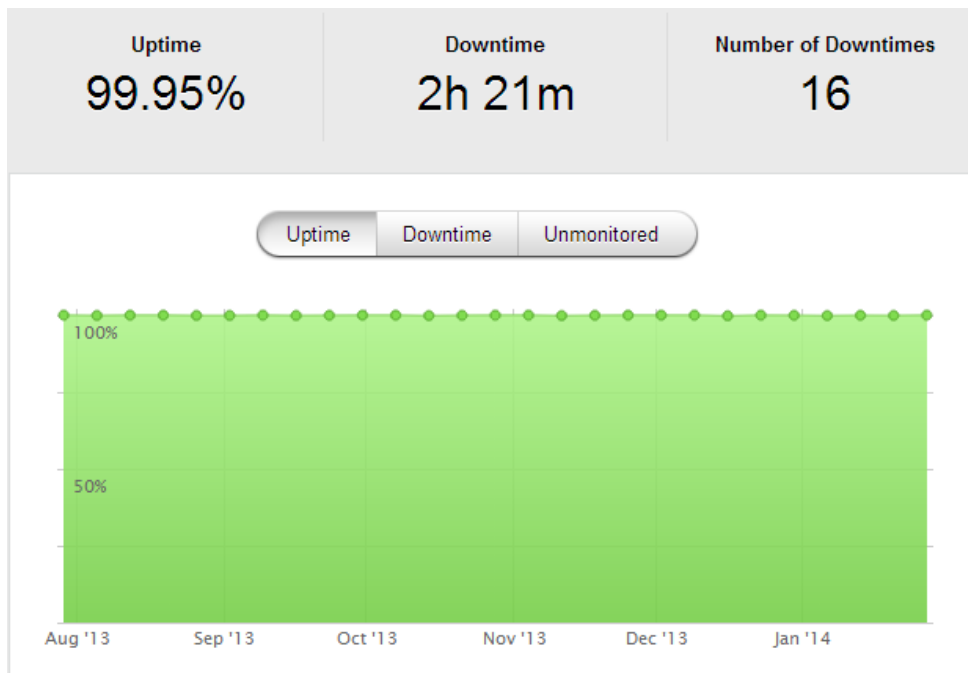
8. Disponibilidad y rendimiento

Los servidores disponen de servicios de alerta que avisan de cualquier problema en el sistema.

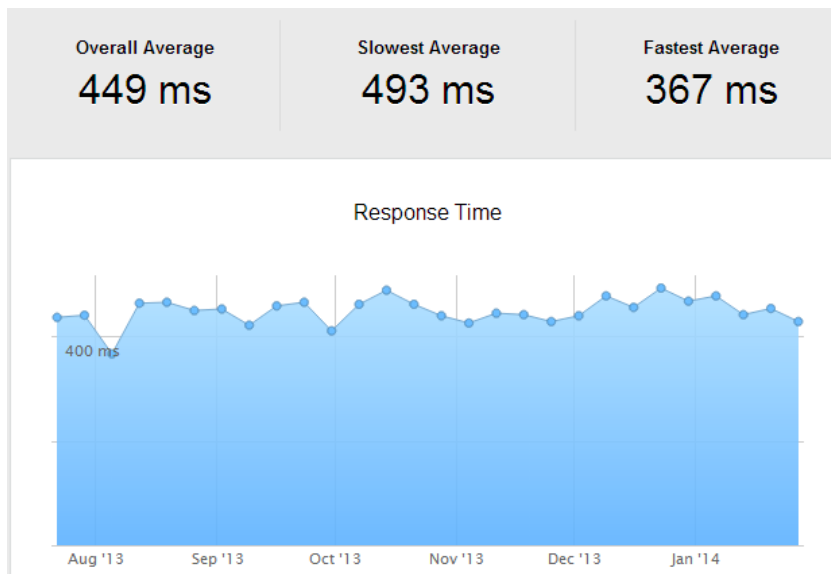
Adicionalmente, un servicio externo monitoriza los servidores y cada cinco minutos comprueba que la plataforma ofrece un servicio correcto, no sólo desde el punto de vista de sistemas sino también a nivel funcional de la aplicación.

Estos servicios, tanto internos como externos, controlan la disponibilidad y el rendimiento del sistema de forma continua avisando de cualquier problema que pueda surgir.

Los datos el último semestre en ITM Platform han sido:



Todas las paradas han sido programadas y sin incidencia en clientes





info@itmplatform.com



www.itmplatform.com