GENERALITAT VALENCIANA
CONSELLERIA D'EDUCACIÓ

Direcció General d'Innovació
Tecnològica Educativa

Av. de Campanar, 32 – 46015 VALÈNCIA
Tel.: 963 18 45 05 – Fax: 963 86 31 75

ITACA - Entrada al sistema ITACA: Describe como entrar al sistema y los problemas típicos asociados al acceso a un sistema informático

Direcció General d'Innovació
Tecnològica Educativa

Av. de Campanar, 32 – 46015 VALÈNCIA
Tel.: 963 18 45 05 – Fax: 963 86 31 75

Índice

Direcció General d'Innovació
Tecnològica Educativa

Av. de Campanar, 32 – 46015 VALÈNCIA
Tel.: 963 18 45 05 – Fax: 963 86 31 75

Entrada al sistema ITACA

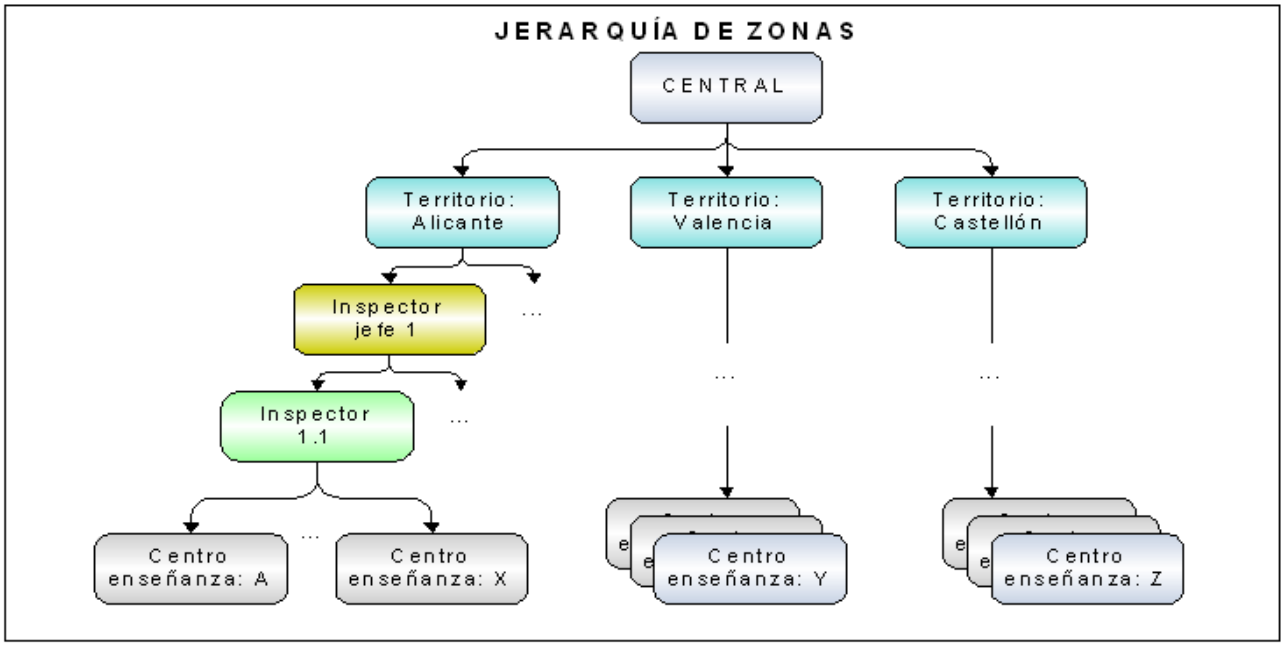
Esta sección describe los mecanismos de seguridad del sistema ITACA para garantizar que cada usuario accede a la información a la que tiene derecho según su puesto y/o cargo y el centro o centros a los que pertenece.
El objetivo del diseño de la seguridad del sistema ITACA es conseguir el máximo grado de descentralización en la gestión y supervisión de los permisos de acceso de los usuarios al sistema garantizando al tiempo la seguridad de los datos del sistema ITACA.
La gestión de los permisos de acceso implica que tipo de perfil (Director, Jefe de Estudios, Docente, Secretaria, etc.) se asigna al usuario. Dentro de cada aplicación y de forma separada se define la funcionalidad a la que accede cada perfil.

Perfiles en el sistema ITACA

El mecanismo de seguridad de ITACA se apoya en los siguientes conceptos:
Usuarios. Se refieren a los usuarios que van a acceder a las aplicaciones. Por ejemplo, Manuel Pellicer.
Perfiles. Indica las posibles funciones que puede realizar un usuario en las aplicaciones del sistema. Por ejemplo, Director.
Zonas. Este objeto expresa un ámbito geográfico. Se utiliza para indicar en qué ámbito geográfico aplica un perfil. Por ejemplo, Centro de enseñanza A.
Ámbito de Actuación (AA). Es un atributo que caracteriza a uno o más usuarios. Puede contener una combinación de un perfil y una zona. Indica qué funciones puede efectuar el usuario sobre qué conjunto de datos.
Los objetos se combinan de la siguiente manera:
Cada usuario puede tener uno o más AA. Por ejemplo, Manuel Pellicer puede ser Jefe de Estudios del centro de enseñanza A y Personal docente en el centro de enseñanza B. En este caso tendrá dos roles: "Jefe Estudios – Centro Enseñanza A" y "Personal docente – Centro de enseñanza B"

Cadena de Responsabilidad. Gestión de Identidad Centralizada en ITACA

La gestión de la identidad o de usuarios del sistema ITACA está por definición centralizada de igual manera que lo están los datos. Sin embargo, el objetivo es que la administración de los usuarios se delegue de forma que cada usuario pueda ser gestionado por su responsable inmediato, favoreciendo la rapidez y facilidad de gestión del amplio colectivo de usuarios del sistema ITACA (cercano a 70.000 usuarios).
Los principios de esta delegación son:
DESCENTRALIZACIÓN:
El responsable de la gestión de los usuarios de cada centro y sus derechos de acceso es el Director.
Los usuarios que estén gestionados en las aplicaciones de personal de la Conselleria (REGPER, BOLSANODOCENTES) se actualizarán automáticamente en ITACA sin necesidad de intervención del responsable del usuario.
El resto de usuarios tendrán que ser gestionados por el Director en ITACA (alta, modificación, baja)
En el caso de los centros de titularidad privada (Concertados, Privados) el propio Director puede tener que ser gestionado por un responsable superior al centro en caso de no pertenecer al colectivo gestionado en las aplicaciones de personal de la Conselleria
ESTRUCTURA DE RESPONSABILIDAD:
El responsable inmediato por encima del Director del Centro es el Inspector. La gestión de aquellos directores no gestionados por Conselleria deberá hacerla el inspector en ITACA (alta, modificación, baja)
El inspector jefe es el supervisor de cada inspector y enlace en la estructura de mando con cada servicio territorial.
La asignación de centros a inspectores se gestiona en la aplicación corporativa ESCOLA sin necesidad de intervención de la estructura de inspección
La siguiente figura muestra gráficamente la estructura de responsabilidad del sistema ITACA:



Reparto de credenciales (usuario/contraseña)

La Conselleria facilitará al usuario el Nombre de usuario (login) y contraseña inicial con la que debe acceder al sistema por primera vez.
La contraseña inicial se puede modificar a través de la Aplicación de Gestión de Identidad descrita en un apartado posterior. El cambio de la contraseña inicial será obligatorio en el primer acceso al sistema en el caso del acceso al entorno de producción del sistema ITACA.

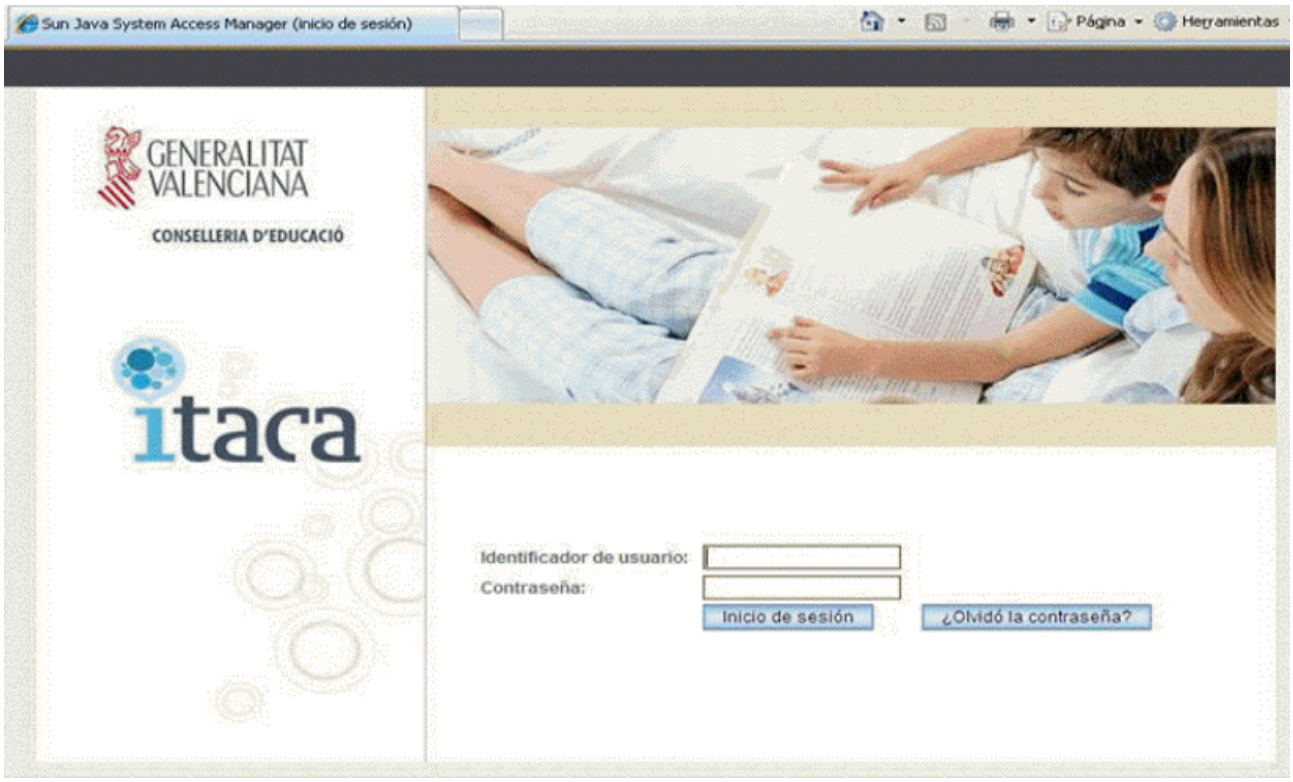
Dirección de acceso al sistema ITACA

La aplicación ITACA tiene una dirección con el esquema https://***Nombre-Servidor***/itaca/Main.html.
El ***Nombre-servidor*** varía en función del entorno al que se acceda (producción o formación):

- En producción el nombre del servidor es itaca.edu.gva.es con lo que la dirección queda: https://itaca.edu.gva.es/itaca/Main.html
- En formación el nombre del servidor es itacaform.edu.gva.es con lo que la dirección queda https://itacaform.edu.gva.es/itaca_form/Main.html

Acceso al sistema ITACA (Login de usuario)

La ventana de acceso al sistema ITACA se muestra a continuación:



En esta ventana el usuario introducirá dos campos:
Nombre del usuario (Login). Coincide con el documento de identidad del usuario (NIF o NIE) completo. El usuario será proporcionado por la Conselleria con la entrega de la credencial de acceso a ITACA:
NIF. Los ocho dígitos más la letra incluyendo **siempre** los dígitos 0 iniciales cuando existan. Por ejemplo el NIF 00324256J tiene que introducirse sin omitir los dos dígitos 0 iniciales
NIE. Compuesto de la letra X de inicio más los 7 dígitos y la letra final incluyendo **siempre** los dígitos iniciales cuando existan. Por ejemplo el NIE X0027456P tiene que introducirse sin omitir los dos dígitos 0 iniciales.
Contraseña: El usuario introducirá la contraseña personal que haya creado siguiendo las reglas que establezca el administrador de la aplicación (por ejemplo, uso de minúscula y mayúscula, números o caracteres de puntuación).
Si el Nombre de usuario y la contraseña son correctos se accederá a las aplicaciones:
Aplicación ITACA. Permite la gestión administrativa del centro y su uso se detalla en el apartado "La aplicación ITACA"
Aplicación de Gestión de Identidad. Permite al usuario la gestión de sus datos personales así como el cambio de contraseña. Además, para aquellos perfiles con responsabilidad en la gestión de usuarios (Director, Inspector) permite la creación, modificación y borrado de usuarios en los centros bajo su responsabilidad. Su uso se describe en el apartado "Aplicación de Gestión de Identidad"

Preguntas personales de acceso

En caso de que el usuario acceda por primera vez al entorno o bien haya olvidado la contraseña actual que posee, el usuario accederá:

- Con el login que se le haya suministrado y pulsando el botón "Olvidé la contraseña" (es decir sin introducir nada en el campo password)

Tras el acceso el sistema lo dirigirá a esta pantalla donde se le preguntarán dos datos personales fijos durante todo el tiempo que tenga usuario de acceso al sistema. En caso de acertar las dos preguntas el usuario pasará a la ventana de cambio de contraseña. En caso de error el sistema le permitirá introducir la respuesta un número de veces configurable hasta que se bloquee su cuenta. En este caso deberá ponerse en contacto con el administrador.
Los datos personales fijos que se le van a preguntar son:

Av. de Campanar, 32 – 46015 VALÈNCIA
Tel.: 963 18 45 05 – Fax: 963 86 31 75

1. Fecha de nacimiento
2. Últimos 6 dígitos de la cuenta bancaria en la que percibe los haberes de la Conselleria (si es un centro público) o los seis dígitos de control de la credencial (si es un centro concertado).

Tras haber contestado acertadamente las dos preguntas, el sistema mostrará la pantalla para el cambio de contraseña. **Una vez cambiada la contraseña, se volverá a la página de login desde donde el usuario podrá entrar ya al sistema con el usuario y contraseña que ha elegido**.

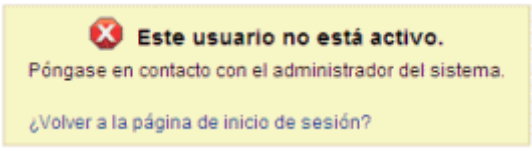
Bloqueo temporal de la cuenta

Como medida de seguridad, el acceso a la cuenta del usuario se bloqueará al cambio de un número de intentos fallidos seguidos (inicialmente 4 intentos). El número de intentos estará administrado por la Conselleria de forma global para todos los usuarios y se podrá modificar durante el uso del sistema
El acceso a la cuenta se bloqueará durante un periodo de tiempo (inicialmente 10 minutos). El objetivo de este bloqueo es evitar que se pueda conseguir acceder a la cuenta de un usuario por otra persona mediante la técnica de averiguar la contraseña mediante intentos repetidos de acceso. De esta manera el número de intentos de acceso que pueda efectuar un extraño diariamente está muy limitado y la posibilidad de averiguar la contraseña desaparece.
La duración del periodo de bloqueo de cuenta también es configurable por la Conselleria.
Tras cada intento de acceso erróneo al autenticarse el número de intentos de acceso fallidos que quedan al usuario para intentar acceder se en obtendrá la siguiente ventana:

Finalizados los intentos se obtendrá un fallo de autenticación en el que se indicará que el usuario no está activo.

Direcció General d'Innovació
Tecnològica Educativa

Av. de Campanar, 32 – 46015 VALÈNCIA
Tel.: 963 18 45 05 – Fax: 963 86 31 75



Una vez expirado el plazo de bloqueo, el usuario volverá a poder acceder a la cuenta con el mismo Nombre de usuario y contraseña que tenía antes de que la cuenta se bloquease. Ni el usuario ni el administrador del sistema tienen que efectuar ninguna acción adicional.