

A DADES DE L'USUARI AUTORITZAT / DATOS DEL USUARIO AUTORIZADO

NOM I COGNOMS / NOMBRE Y APELLIDOS	DNI / NIE	CENTRE / CENTRO
USUARI / USUARIO	NÚMERO DE CONTROL	

B COMPROMÍS / COMPROMISO

1. És obligació de l'usuari modificar la contrasenya la primera vegada que accedix a l'aplicació ÍTACA.
Es obligación del usuario modificar la contraseña la primera vez que accede a la aplicación ÍTACA.
2. L'usuari ha de mantindre les seues claus d'accés i mai ha de facilitar a ningú la contrasenya d'accés ni usar les d'altres.
El usuario debe mantener sus claves de acceso y nunca debe facilitar a nadie la contraseña de acceso ni usar las de otros.
3. Notificar al responsable de l'aplicació quan el secret de la seua contrasenya s'haja vist compromés.
Notificar al responsable de la aplicación cuando el secreto de su contraseña se haya visto comprometido.
4. És obligatori tancar l'aplicació quan s'abandone el lloc de treball.
Es obligatorio cerrar la aplicación cuando se abandone el puesto de trabajo.
5. És obligatori comunicar al responsable de l'aplicació les revocacions d'accés per canvis en les funcions que realitza l'usuari, quan no siguen necessàries.
Es obligatorio comunicar al responsable de la aplicación las revocaciones de acceso por cambios en las funciones que realiza el usuario, cuando no sean necesarias.
6. Està prohibit copiar la informació a l'ordinador personal, disquets o a qualsevol altre suport sense autorització expressa del responsable de l'aplicació.
Está prohibido copiar la información al ordenador personal, disquetes o a cualquier otro soporte sin autorización expresa del responsable de la aplicación.
7. No es permet introduir o crear fitxers que continguen dades de caràcter personal sense que prèviament hagen siguts autoritzats en la forma reglamentàriament prevista.
No se permite introducir o crear ficheros que contengan datos de carácter personal sin que previamente hayan sido autorizados en la forma reglamentariamente prevista.
8. En tot cas, les dades de caràcter personal objecte de tractament automatitzat degudament autoritzat no es podran usar per a finalitats distintes d'aquelles per a les quals hagen sigut obtingudes.
En todo caso, los datos de carácter personal objeto de tratamiento automatizado debidamente autorizado no se podrán usar para finalidades distintas de aquellas para las que hayan sido obtenidos.
9. Només es podrà fer ús dels recursos i sistemes a què s'haja autoritzat expressament l'accés i només per al desenvolupament de les funcions encomanades legítimament i de les tasques derivades; queda, per tant, prohibit l'ús dels sistemes o els recursos de la Generalitat i les entitats i organismes que la componen per a fins particulars, així com l'ús de recursos o sistemes no autoritzats.
Solamente se podrá hacer uso de los recursos y sistemas a los que se haya autorizado expresamente el acceso y solamente para el desarrollo de las funciones encomendadas legítimamente y de sus tareas derivadas; queda, por tanto, prohibido el uso de los sistemas o los recursos de la Generalitat y las entidades y organismos que la componen para fines particulares, así como el uso de recursos o sistemas no autorizados.
10. Tant l'eixida de suports, com l'accés remot i la còpia de dades de caràcter personal, serà autoritzada només per la persona responsable dels fitxers corresponents, adoptant les mesures tendents a impedir qualsevol recuperació indeguda d'informació, xifrant les dades quan es tracte de fitxers de nivell alt de protecció (que continguen informació sobre ideologia, religió, creences, afiliació sindical, origen racial o ètnic, salut o vida sexual).
Tanto la salida de soportes, como el acceso remoto y la copia de datos de carácter personal, de uso en la Conselleria, será autorizada sólo por la persona responsable de los ficheros correspondientes, adoptando las medidas tendentes a impedir cualquier recuperación indebida de información, cifrando los datos cuando se trate de ficheros de nivel alto de protección (que contengan información sobre ideología, religión, creencias, afiliación sindical, origen racial o étnico, salud o vida sexual).

C NORMES PARTICULARS DE SEURETAT / NORMAS PARTICULARES DE SEGURIDAD

1. Per a poder accedir a les aplicacions haurà de teclejar-se la contrasenya personal i intransferible.
Para poder acceder a las aplicaciones deberá teclearse la contraseña personal e intransferible.
2. La contrasenya haurà de tindre un mínim de vuit caràcters (almenys 2 numèrics i altres 2 alfabètics).
La contraseña deberá tener un mínimo de ocho caracteres (al menos 2 numéricos y otros 2 alfabéticos).
3. No està permès l'ús de claus compartides o multiusuaris.
No está permitido el uso de claves compartidas o multiusuarios.
4. Periòdicament, el sistema avisarà perquè canvie la contrasenya.
Periódicamente, el sistema avisará para que cambie la contraseña.
5. Quan teclege la contrasenya, no es mostraran els caràcters.
Cuando teclee la contraseña, no se mostrarán los caracteres.
6. La sessió es desconnectarà després d'un temps sense utilitzar l'aplicació.
La sesión se desconectará después de un tiempo sin utilizar la aplicación.
7. Es revisaran periòdicament els drets d'accés a l'aplicació.
Se revisarán periódicamente los derechos de acceso a la aplicación.
8. El registre dels fitxers amb dades de caràcter personal correspon al responsable de les dades, que serà el centre directiu.
El registro de los ficheros con los datos de carácter personal corresponde al responsable de los datos, que será el centro directivo.

D ACCEPTACIÓ / ACEPTACIÓN

Amb la seua firma, la persona usuària del sistema manifesta la comprensió i acceptació de les condicions d'accés i es compromet a complir la normativa vigent en matèria de seguretat informàtica i protecció de dades de caràcter personal.
Quan els canvis en les condicions de seguretat ho aconsellen, s'emetrà una nova credencial.

*Con su firma, la persona usuaria del sistema manifiesta la comprensión y aceptación de las condiciones de acceso y se compromete a cumplir la normativa vigente en materia de seguridad informática y protección de datos de carácter personal.
Cuando los cambios en las condiciones de seguridad lo aconsejen, se emitirá una nueva credencial.*

_____, _____ d _____ de _____

Firma de l'usuari / Firma del usuario

A DADES DE L'USUARI AUTORITZAT / DATOS DEL USUARIO AUTORIZADO

NOM I COGNOMS / NOMBRE Y APELLIDOS	DNI / NIE	CENTRE / CENTRO
USUARI / USUARIO	NÚMERO DE CONTROL	

B COMPROMÍS / COMPROMISO

1. És obligació de l'usuari modificar la contrasenya la primera vegada que accedix a l'aplicació ÍTACA.
Es obligación del usuario modificar la contraseña la primera vez que accede a la aplicación ÍTACA.
2. L'usuari ha de mantindre les seues claus d'accés i mai ha de facilitar a ningú la contrasenya d'accés ni usar les d'altres.
El usuario debe mantener sus claves de acceso y nunca debe facilitar a nadie la contraseña de acceso ni usar las de otros.
3. Notificar al responsable de l'aplicació quan el secret de la seua contrasenya s'haja vist compromés.
Notificar al responsable de la aplicación cuando el secreto de su contraseña se haya visto comprometido.
4. És obligatori tancar l'aplicació quan s'abandone el lloc de treball.
Es obligatorio cerrar la aplicación cuando se abandone el puesto de trabajo.
5. És obligatori comunicar al responsable de l'aplicació les revocacions d'accés per canvis en les funcions que realitza l'usuari, quan no siguen necessàries.
Es obligatorio comunicar al responsable de la aplicación las revocaciones de acceso por cambios en las funciones que realiza el usuario, cuando no sean necesarias.
6. Està prohibit copiar la informació a l'ordinador personal, disquets o a qualsevol altre suport sense autorització expressa del responsable de l'aplicació.
Está prohibido copiar la información al ordenador personal, disquetes o a cualquier otro soporte sin autorización expresa del responsable de la aplicación.
7. No es permet introduir o crear fitxers que continguen dades de caràcter personal sense que prèviament hagen siguts autoritzats en la forma reglamentàriament prevista.
No se permite introducir o crear ficheros que contengan datos de carácter personal sin que previamente hayan sido autorizados en la forma reglamentariamente prevista.
8. En tot cas, les dades de caràcter personal objecte de tractament automatitzat degudament autoritzat no es podran usar per a finalitats distintes d'aquelles per a les quals hagen sigut obtingudes.
En todo caso, los datos de carácter personal objeto de tratamiento automatizado debidamente autorizado no se podrán usar para finalidades distintas de aquellas para las que hayan sido obtenidos.
9. Només es podrà fer ús dels recursos i sistemes a què s'haja autoritzat expressament l'accés i només per al desenvolupament de les funcions encomanades legítimament i de les tasques derivades; queda, per tant, prohibit l'ús dels sistemes o els recursos de la Generalitat i les entitats i organismes que la componen per a fins particulars, així com l'ús de recursos o sistemes no autoritzats.
Solamente se podrá hacer uso de los recursos y sistemas a los que se haya autorizado expresamente el acceso y solamente para el desarrollo de las funciones encomendadas legítimamente y de sus tareas derivadas; queda, por tanto, prohibido el uso de los sistemas o los recursos de la Generalitat y las entidades y organismos que la componen para fines particulares, así como el uso de recursos o sistemas no autorizados.
10. Tant l'eixida de suports, com l'accés remot i la còpia de dades de caràcter personal, serà autoritzada només per la persona responsable dels fitxers corresponents, adoptant les mesures tendents a impedir qualsevol recuperació indeguda d'informació, xifrant les dades quan es tracte de fitxers de nivell alt de protecció (que continguen informació sobre ideologia, religió, creences, afiliació sindical, origen racial o ètnic, salut o vida sexual).
Tanto la salida de soportes, como el acceso remoto y la copia de datos de carácter personal, de uso en la Conselleria, será autorizada sólo por la persona responsable de los ficheros correspondientes, adoptando las medidas tendentes a impedir cualquier recuperación indebida de información, cifrando los datos cuando se trate de ficheros de nivel alto de protección (que contengan información sobre ideología, religión, creencias, afiliación sindical, origen racial o étnico, salud o vida sexual).

C NORMES PARTICULARS DE SEURETAT / NORMAS PARTICULARES DE SEGURIDAD

1. Per a poder accedir a les aplicacions haurà de teclejar-se la contrasenya personal i intransferible.
Para poder acceder a las aplicaciones deberá teclearse la contraseña personal e intransferible.
2. La contrasenya haurà de tindre un mínim de vuit caràcters (almenys 2 numèrics i altres 2 alfabètics).
La contraseña deberá tener un mínimo de ocho caracteres (al menos 2 numéricos y otros 2 alfabéticos).
3. No està permès l'ús de claus compartides o multiusuaris.
No está permitido el uso de claves compartidas o multiusuarios.
4. Periòdicament, el sistema avisarà perquè canvie la contrasenya.
Periódicamente, el sistema avisará para que cambie la contraseña.
5. Quan teclege la contrasenya, no es mostraran els caràcters.
Cuando teclee la contraseña, no se mostrarán los caracteres.
6. La sessió es desconnectarà després d'un temps sense utilitzar l'aplicació.
La sesión se desconectará después de un tiempo sin utilizar la aplicación.
7. Es revisaran periòdicament els drets d'accés a l'aplicació.
Se revisarán periódicamente los derechos de acceso a la aplicación.
8. El registre dels fitxers amb dades de caràcter personal correspon al responsable de les dades, que serà el centre directiu.
El registro de los ficheros con los datos de carácter personal corresponde al responsable de los datos, que será el centro directivo.

D ACCEPTACIÓ / ACEPTACIÓN

Amb la seua firma, la persona usuària del sistema manifesta la comprensió i acceptació de les condicions d'accés i es compromet a complir la normativa vigent en matèria de seguretat informàtica i protecció de dades de caràcter personal.
Quan els canvis en les condicions de seguretat ho aconsellen, s'emetrà una nova credencial.

*Con su firma, la persona usuaria del sistema manifiesta la comprensión y aceptación de las condiciones de acceso y se compromete a cumplir la normativa vigente en materia de seguridad informática y protección de datos de carácter personal.
Cuando los cambios en las condiciones de seguridad lo aconsejen, se emitirá una nueva credencial.*

_____, _____ d _____ de _____

Firma de l'usuari / Firma del usuario