ANEXO 4

PROTECCIÓN DE DATOS

- Introducción
- Manual de uso

INTRODUCCIÓN

Para poder garantizar el cumplimiento del Reglamento General De Protección de Datos (UE) 2016/679 y leyes complementarias, se ha implementado el *Módulo de Protección de Datos*, donde un administrador puede controlar los usuarios que harán uso de Ergo/IBV.

Este sistema de control de accesos puede ser configurable por el administrador de la manera más conveniente:

- Permite implantar el mecanismo de autenticación con usuario y contraseña en Ergo/IBV, identificando de forma inequívoca y personalizada al usuario que acceda al módulo de *Diseño antropométrico del puesto de trabajo*.
- Mantiene un registro de accesos al módulo de *Diseño antropométrico del puesto de trabajo* y a los datos de los trabajadores.
- Tiene la posibilidad de limitar el número de reintentos de acceso no autorizados a la aplicación.
- Permite establecer un tiempo de validez de las contraseñas, transcurrido el cual éstas caducan y los usuarios son instados a cambiarlas

MANUAL DE USO

Este manual de uso está dirigido al administrador de sistemas o personal técnico equivalente. Por defecto la base de datos con la que trabaja el módulo de protección de datos es *ModuloPD.mdb* y está ubicada en el directorio de la aplicación, pero puede renombrarse y ubicarse donde se desee, indicándolo en el fichero de configuración *'ModuloPD.ini'* que se encuentra en la carpeta *Config* del directorio de instalación de Ergo/IBV.

Para entrar en el *Módulo de Protección de Datos*, debe ejecutar el archivo *ModuloPD.exe* ubicado en el directorio de la aplicación, inmediatamente se despliega un cuadro de diálogo (Figura 1) donde deberá introducir el usuario y la contraseña del administrador. Inicialmente, puede entrar con:

Usuario: ***administrador***

Contraseña: ***admin***

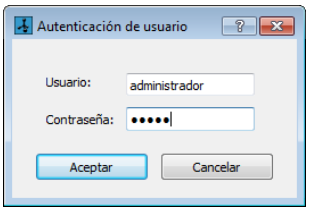

Figura 1. Identificación del administrador

Después de realizar la autenticación correctamente, aparece la ventana principal de la aplicación (Figura 2). Deberá establecer una nueva contraseña de administrador [ver apartado "*Cambio contraseña*", en el presente capítulo].

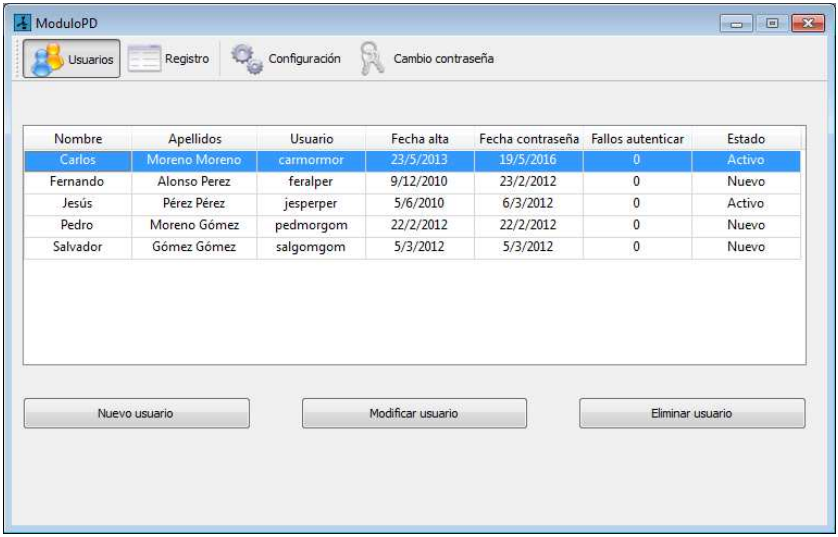

Figura 2. Ventana principal

En la zona superior de la ventana principal encontramos una barra de herramientas con las siguientes opciones:

Usuarios. Accede a la gestión de usuarios de Ergo/IBV.

Registro. Visualiza el registro de actividad de los usuarios.

Configuración. Permite configurar la protección de datos.

Cambio contraseña. Permite cambiar la contraseña del administrador.

Cómo activar el control de accesos

Para activar el sistema de control de accesos en Ergo/IBV debe seguir los siguientes pasos:

1. Pulsar el botón **Configuración**, en la ventana que aparece activar la casilla '*Habilitar control de acceso a la aplicación'* y pulsar el botón *Aceptar*.
2. Pulsar el botón **Usuarios**, Haciendo uso del botón *Nuevo usuario*, crear todos los usuarios que deban acceder a la aplicación.

A partir de este momento sólo los usuarios creados podrán ejecutar Ergo/IBV, y para ello tendrán que hacer uso de su correspondiente usuario y contraseña. Además, todas las lecturas y escrituras que realicen quedarán almacenadas en un registro de actividad.

Gestión de Usuarios

Pulsando el botón *Usuarios* se muestra una tabla con todos los usuarios del módulo (Figura 2) donde para cada usuario se muestra: nombre, apellidos, usuario, fecha alta, fecha contraseña, fallos autenticación y estado.

En la parte inferior dispone de tres botones:

Nuevo usuario. Permite crear un nuevo usuario, despliega una nueva ventana donde se debe introducir sus datos (Figura 3):

Nombre y *Apellidos.*

Usuario: debe tener como mínimo 8 caracteres alfanuméricos.

Contraseña: debe tener como mínimo 6 caracteres en total, entre ellos 2 numéricos.

Fecha de Alta: por defecto será la fecha actual.

Estado: Refleja el estado de la cuenta de usuario, por defecto tiene valor establecido a *Nuevo.* Puede tener tres valores:

- *Nuevo*: Este estado se mantendrá mientras el usuario no cambie su contraseña. Al hacer la autenticación, se le permite el acceso pero será informado de su estado y de la necesidad de cambiar su contraseña.
- *Activo*: es el estado que indica que el usuario está habilitado para utilizar Ergo/IBV. Al identificarse correctamente se le permitirá el acceso de Ergo/IBV.
- *Bloqueado*: en este estado al usuario se le deniega el acceso a la aplicación. Puede asignarlo el administrador o también puede ser asignado automáticamente cuando el usuario supera el número de reintentos fallidos de autenticación.
- *Fallos Autenticar*: indica el número de intentos fallidos de autenticación de forma consecutiva. Inicialmente será cero, el sistema contabilizará los intentos fallidos y restaurará el valor a cero cuando se produzca una autenticación positiva.

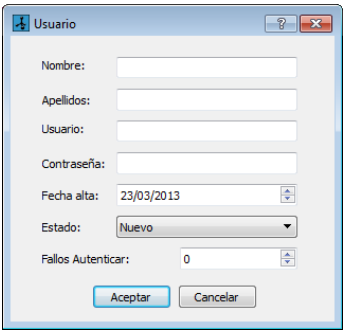

Figura 3. Ficha de usuario

Modificar usuario. Permite modificar los datos del usuario seleccionado en la lista. Se desplegará la ficha de usuario con sus datos que podrán editar.

Eliminar usuario. Permite borrar el usuario seleccionado pidiendo antes confirmación.

Registro de Actividad

Como ya se ha comentado, si se habilita el *Control de acceso a la aplicación,* la aplicación IBV registrará la actividad de los usuarios que la ejecuten [ver apartado *"Configuración"*, en el presente capítulo]. Para ello se escribirán en un fichero de base de datos los accesos a la aplicación y las acciones de lectura y escritura sobre datos de trabajadores.

Cuando un usuario se intenta autenticar, se crea un registro indicando un acceso de autentificación, el usuario que la realiza, la fecha y la hora en que se realiza y si el acceso ha sido autorizado o denegado.

Cuando el usuario abre o guarda puestos de trabajo, se genera un registro de acceso a los datos que indicará: el usuario, la fecha y la hora en que se realiza, el archivo accedido, el tipo de acceso (lectura, escritura, borrado, creación, importación o exportación) y si ha sido autorizado o denegado (siempre autorizado).

Si pulsamos el botón **Registro** de la barra de herramientas se mostrará una tabla con todos los registros de actividad generados por el uso de la aplicación.

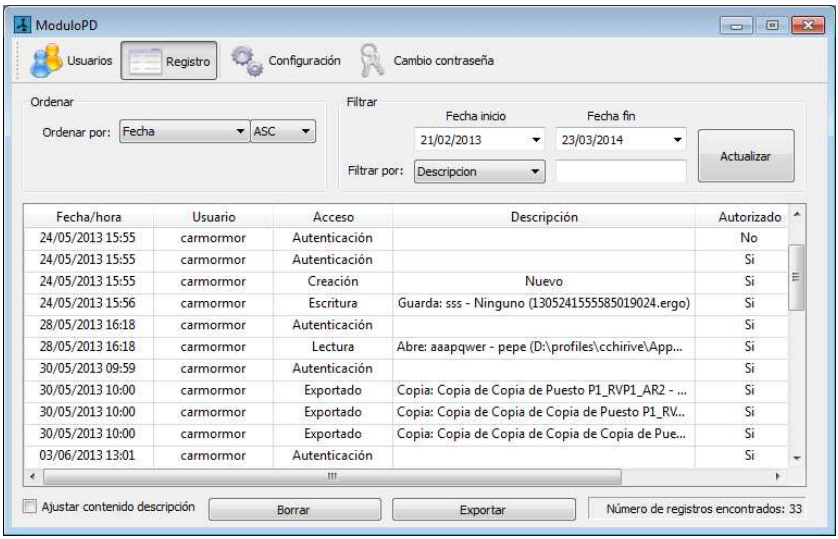

Figura 4. Registro de actividad

Sobre esa tabla podrá realizar las siguientes acciones sobre los registros de actividad:

Ordenar. Para ello debe seleccionar en el primer desplegable el campo de ordenación (usuario, fecha, acción, etc.) y en el segundo desplegable si desea ordenación ascendente o descendente (ASC o DESC).

Filtrar: Cada vez que cambie las opciones de filtrado será necesario que pulse el botón *Actualizar* para que se refresque la lista de registros. Se puede filtrar registros de la siguiente manera:

- Por fecha: registros entre *Fecha inicio* y *Fecha fin*.
- Por otro campo: para ello debe seleccionar en el desplegable '*Filtrar por*' el campo por el que se desea filtrar:
    - Si selecciona *Usuario, Acceso* o *Autorizado*, se cargarán en un segundo desplegable los valores posibles para dicho campo de forma que solo tenga que seleccionar el valor de filtro deseado.
    - Si selecciona *descripción*, se podrá introducir texto libre y se filtrarán las acciones que contengan el texto indicado.

Borrar. Esta opción elimina los registros listados, es decir, los que cumplen los criterios de filtrado.

Por ejemplo si usted quisiera eliminar todos los registros no autorizados de un periodo dado, debería seleccionar la fecha de inicio y fin del periodo deseado y seleccionar en el desplegable de filtrado el campo Autorizado y en el segundo desplegable, la opción No. Al pulsar el botón de Actualizar se mostrarían los registros que cumplen ese criterio y ya podría borrarlos.

Al pulsar el botón de borrado se muestra un mensaje de confirmación y si la respuesta es positiva se muestra un mensaje recomendando al administrador que antes del borrado es conveniente que exporte los registros a fichero y dando oportunidad de hacerlo.

Exportar. Permite exportar los registros listados, es decir, los que cumplen los criterios de filtrado, a un fichero con formato estructurado CSV.

Configuración

Para configurar el módulo de protección de datos, en la pantalla principal debe pulsar el botón *Configuración,* entonces aparecerá una pantalla que permite configurar los parámetros de este control de acceso (Figura 5).

La casilla de verificación *Habilitar control de acceso a la aplicación*, permite habilitar o deshabilitar la actividad del módulo de protección de datos en Ergo/IBV. Si habilita el control, la aplicación IBV pedirá autenticación al comienzo de su ejecución y registrará la actividad de los usuarios que la utilicen. Si deshabilita el control no hará ninguna de las dos cosas. Tras la instalación de Ergo/IBV este control está deshabilitado, hasta que es habilitado por el administrador.

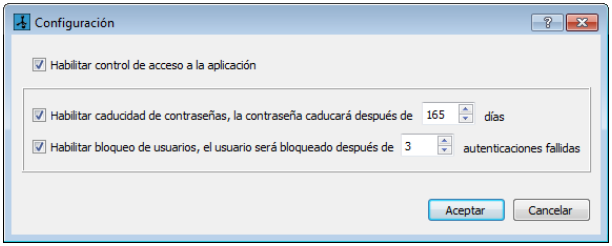

Figura 5. Ventana de configuración

La casilla de verificación *Habilitar caducidad de contraseñas*, permite habilitar o deshabilitar la funcionalidad de que las contraseñas caduquen de forma automática transcurrido un periodo de tiempo después de haberla establecido. Si se habilita, es posible configurar el número de días durante los que es válida una contraseña. Cuando una contraseña caduca, el usuario puede acceder a Ergo/IBV, pero ésta le recuerda que debe cambiar la contraseña.

La casilla de verificación *Habilitar bloqueo de usuarios*, permite habilitar o deshabilitar la funcionalidad de que los usuarios pasen a estado bloqueado de forma automática si alcanzan el número máximo de autentificaciones fallidas permitido. Si se habilita, es posible configurar ese número máximo de intentos permitido. Cuando un usuario se bloquea, ya no podrá acceder a la aplicación hasta que el administrador lo desbloquee.

Cambio contraseña

Si pulsa el botón Cambio contraseña podrá modificar la contraseña del administrador, para ello deberá introducir la contraseña actual seguida de la nueva y su confirmación.

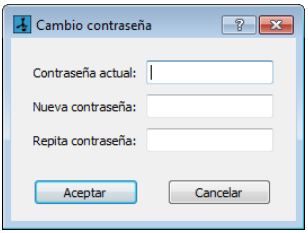

Figura 6. Cambio de contraseña