Normas de seguridad de acceso a las aplicaciones

CAI y SEU

A continuación se describen las obligaciones de los usuarios que tienen acceso a aplicaciones que contienen datos de carácter personal.

Estas normas de seguridad se aplican a las aplicaciones siguientes:

- CAI: Aplicación de gestión de incidencias en el sistema informático de la CAIB
- SEU: Sistema de seguridad y control informático de la CAIB

Es necesario leer las dichas obligaciones y firmar la hoja adjunta en la cual se acepta el conocimiento y la obligación de cumplir dichas normas.

Puestos de trabajo

Cada puesto de trabajo estará bajo la responsabilidad de un usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Cuando un usuario abandona su puesto de trabajo, bien temporalmente o bien al finalizar su jornada laboral, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de los ficheros, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones y sistemas operativos, que solo podrá ser modificada bajo la autorización del Responsable de Seguridad Técnico.

Salvaguarda y protección de las contraseñas personales

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

Gestión de incidencias

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad de los ficheros, tanto automatizados como no automatizados, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad.

Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al Registro de incidencias.

El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad de los ficheros por parte de ese usuario.

Procedimiento de notificación de incidencias

Cualquier usuario que tenga conocimiento de una incidencia es responsable de su notificación. Esta notificación puede realizarse de la siguiente manera:

Por mail: remitiendo el Formulario de Aviso de Incidencias a la dirección de correo seguretat@dgtic.caib.es