Funciones y obligaciones que afectan a los usuarios del fichero de "Gestión Telefónica" de la UPV

El personal autorizado a acceder a la información de carácter personal del Fichero, realizará las funciones propias de su puesto de trabajo, que se encuentran previstas en las relaciones de puestos de trabajo del Centro o Unidad Administrativa a la que pertenezca, a la correspondiente definición de funciones que se aplique a dicho personal.

Además de dichas funciones relativas al desempeño profesional asociado a su puesto laboral, todo el personal colaborará con el Responsable Interno del Fichero y Encargado Interno del Tratamiento en pro de velar por el cumplimiento de la legislación y reglamentación vigente sobre Protección de Datos de Carácter Personal.

- Guardar secreto profesional y confidencialidad de la información tratada. Quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.
- La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos personales será considerado como una falta leve, grave o muy grave de conformidad con lo previsto en el artículo 44 de la LOPD, lo cual dará lugar a iniciación de actuaciones disciplinarias, si procediesen.
- Utilizar los sistemas de información, recursos técnicos así como la información personal a la que se accede, únicamente para el desarrollo y desempeño profesional que el usuario tiene asignado.
- Facilitar el derecho de acceso, rectificación y cancelación a los titulares de los datos. Para ello se informará inmediatamente al Responsable del Fichero Responsable de Seguridad o Encargado del tratamiento y se recogerá siempre en solicitud escrita.
- 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 inmediatamente a su cambio.
- Cada usuario deberá cambiar la contraseña inicial que se le asigne, en el primer acceso que realice al sistema o tras el desbloqueo de su contraseña cuando haya sido necesaria la intervención de una tercera persona en dicho proceso. Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento etc.
- Para ello se seguirán las pautas de la Política de Contraseñas de la Universidad Politécnica de Valencia para la elección de las contraseñas.
- Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.
- 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 el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos, como por ejemplo un protector de pantalla con contraseña. 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 Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a redes o sistemas exteriores, que no esté autorizado expresamente por el Responsable del Fichero o el Director del Centro o departamento al que pertenezca cada usuario. La revocación de esta prohibición deberá ser autorizada expresamente
- Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo la autorización de los administradores autorizados del **Anexo F.**
- Cuando se realicen tratamientos de datos extraídos del Fichero, con programas ofimáticos, como procesadores de texto u hojas de cálculo, deberá ser comunicarlo para su aprobación al Encargado Interno del Tratamiento para que se proceda a implantar las medidas de seguridad adecuadas. La utilización de dichos programas para el tratamiento de datos personales sin comunicarlo al Encargado Interno del Tratamiento será considerado como una falta contra la seguridad del fichero por parte de ese usuario.
- Se deberá evitar el guardar copias de los datos personales del Fichero en archivos intermedios o temporales. En el caso de que sea imprescindible realizar esas copias temporales por exigencias del tratamiento, se deberán adoptar las siguientes precauciones:
    - Realizar siempre esas copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por todo el disco del ordenador y siempre se pueda conocer dónde están los datos temporales.
    - Tras realizar el tratamiento para los que han sido necesarios esos datos temporales, proceder al borrado o destrucción de los mismos.
    - Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de Medidas de Seguridad.
- Trabajo fuera de los locales de ubicación del fichero. No se deberá copiar ni transportar información de los sistemas centrales en portátiles o estaciones de trabajo que se encuentren fuera de las oficinas sin la correspondiente autorización del Encargado Interno del Fichero. En el **Anexo G** se referencia un procedimiento para el tratamiento de ficheros fuera de su ubicación, como es el caso de los ordenadores portátiles.
- Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al Encargado Interno del Fichero o a la persona encargada de registrarla. El modelo de notificación de incidencias figura en el **Anexo I.**
- El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.
- Todos los usuarios estarán obligados a guardar el secreto profesional y el deber de custodia respecto de los datos de carácter personal a los que tengan acceso en el desempeño de su función aún después de haber abandonado la universidad.
- Cuando un usuario gestione o produzca soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, estos deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.
- Cuando se reciclen medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables. Aquellos que no vayan a ser reutilizados deberán ser destruidos mediante un procedimiento especificado en el **Anexo G**.

- Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero.
- La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero. mediante el procedimiento descrito en el **Anexo G**.
- Solo se podrán realizar envíos del Fichero, por correo electrónico o transferencias electrónicas, desde una única cuenta o dirección de correo controlado por un usuario especialmente autorizado por el Encargado Interno del Tratamiento o persona autorizada tal como se describe en el **Anexo G.**

Anexo F Nombramientos y autorizaciones

Nombramientos

Encargado interno del tratamiento: Marta Monléon Alegre.

Administradores del sistema:

- Jorge Ignacio Jover Bou.

- Administradores del sistema designados por el ASIC para el desarrollo de sus funciones.

Otras autorizaciones:

- Responsables que puedan autorizar consultas, altas, bajas , modificaciones del fichero: Ciertos usuarios el sistema (gestores de centro de facturación) tienen autorización para delegar en otros usuarios de su elección.
- Responsables de Salida Soportes: Los administradores de seguridad designados por el ASIC.
- Responsables de Salida por Red: Los administradores de seguridad designados por el ASIC.

Autorizaciones de accesos a Usuarios

Los usuarios autorizados para el acceso al fichero, el perfil de acceso y los recursos a los que tiene acceso se relaciona en la tabla TEL_PERMISOS, donde se mantiene actualizada dicha información. La fecha de alta y/o fecha de baja y la persona que autoriza se relaciona en la tabla TEL_ACCESOS, donde se mantiene actualizada dicha información.

Anexo G. Procedimientos de control y seguridad

G.1 Procedimiento para dar altas, baja o modificación de acceso a usuarios

El alta de usuarios de perfil Gestor de Centro de Facturación Telefónica (CFT) se realizará a través de la aplicación de Gestión Telefónica por otro usuario de perfil Gestor del mismo CFT; o mediante carta firmada por el responsable máximo de la entidad correspondiente al CFT dirigida al servicio de Infraestructuras. Los usuarios con perfil Supervisor, o con perfil Gestor con ámbito de la UPV serán autorizados por el Servicio de Infraestructuras. La baja de usuarios se realiza mediante los mismos mecanismos.

Las autorizaciones realizadas a través de la aplicación de Gestión Telefónica se consideran implícitamente aprobadas por el Encargado Interno del Tratamiento.

G.2 Procedimiento de control de identificación y autenticación

El mecanismo de identificación y autenticación es implementado mediante el sistema de acceso de la intranet UPV, cuya responsabilidad y gestión pertenece al ASIC. La política de establecimiento de claves en la UPV se encuentra en los documentos correspondientes.

G.3 Procedimiento de respaldo y recuperación.

El procedimiento de respaldo y recuperación, la frecuencia de respaldo y el tipo de soporte es responsabilidad del ASIC en el desarrollo de sus funciones.

G.4 Procedimiento de gestión de soportes

El procedimiento de gestión de soportes es responsabilidad del ASIC en el desarrollo de sus funciones. La información de identificación de etiquetas, inventario de soportes, lugar de almacenamiento, registro de respaldos, frecuencia y métodos de borrado físico para reutilización de soportes es mantenida por el ASIC.

G.5 Procedimiento de gestión de salida de soportes

El registro de autorizaciones de salida de soportes es gestionado por el ASIC en el desarrollo de sus funciones, manteniendo la información de fecha y hora de la salida del soporte; tipo, número, contenido, ficheros y fecha de creación del soporte; finalidad, destino y destinatario de la salida; medio de envío, remitente y precauciones de transporte; responsable de la entrega, nombre, cargo y firma de la persona que autoriza. En el caso de entradas y salidas por red se especifica cuenta de correo autorizadas para enviar y responsable de transferencias electrónicas.

G.6 Procedimiento para la destrucción de desechos informáticos

Procedimiento para la destrucción de desechos informáticos

Todos los desechos informáticos de cualquier tipo que puedan contener información del Fichero, como CDs, cintas, discos removibles, listados, memorias removibles de cualquier tipo, o incluso los propios ordenadores obsoletos que contengan discos e almacenamiento, deberán ser eliminados o destruidos de acuerdo con el siguiente Procedimiento para la Destrucción de Desechos Informáticos.

1. Como norma general ningún desecho informático, ya sea listado u otro tipo de soporte, debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

2. Aquellos informes en papel o CDs que contengan datos de carácter personal más sensible y no sean voluminosos, deberán ser destruidos en una destructora de papel si es que existe en la organización.

3. En caso de no existir máquina destructora de papel y CDs o en el caso de que los listados e informes sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una compañía de reciclaje que garantice mediante contrato la destrucción de los mismos.

4. Todos los disquetes y otros soportes removibles desechados deberán ser formateados y entregados para su reutilización al Encargado Interno del Tratamiento. En el caso de que no se vayan a reutilizar deberán ser formateados si se puede, y depositados en los Contenedores confidenciales de la organización para ser entregadas a la empresa encarga da de la destrucción de los datos.

5. Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras instituciones, deberá comunicarse al Encargado Interno del Tratamiento para que se formatee el disco duro o se pase un programa especial que elimine de forma segura todos los datos de los discos duros. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y depositarlos en el Contenedor de la empresa de reciclaje para su destrucción.

6. El Encargado Interno del Tratamiento deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

G.7 Autorización para el uso de PC portátiles

Se indicarán a continuación las autorizaciones realizadas por el Encargado Interno del Tratamiento para el uso de portátiles fuera de las dependencias de la UPV con datos del fichero. Se adjuntarán a este documento las autorizaciones expresas, indicando la persona autorizada, la identificación del equipo, el fichero o los datos que contiene, y las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o, pérdida del equipo.

G.8 Sistemas de cifrado de datos.

No se utilizan sistemas específicos para el cifrado de los datos del fichero.

Anexo I. Notificación y Gestión de incidencias

Procedimiento de Notificación de incidencias

Cuando ocurra una incidencia, el usuario o el administrador, deberá comunicarla al Encargado Interno del Tratamiento o al Responsable del fichero o superior inmediato, para que procedan a su registro en el Libro que habrá habilitado a tal efecto.

En cualquier caso una notificación de incidencia deberá hacer constar:

Tipo de incidencia

Fecha y hora en que se produjo

Persona que realiza la notificación

Persona a quien se comunica

Descripción detallada de la misma

Efectos que puede producir la incidencia, si se conocen o presumen

Se adjunta un ejemplo de impreso de notificación de incidencias.

Procedimiento de gestión de incidencias

El responsable de analizar el registro de incidencias y de decidir, registrar y aplicar las medidas correctoras que se tomen en cada caso es el **Encargado Interno del Tratamiento**.

Impreso de notificación de incidencias

Incidencia Nº: **|**_____**|** (Este número será rellenado por el Responsable de seguridad)
Fecha de notificación: **/**__**/**__**/**_____**/**
Tipo de incidencia**:**
Descripción detallada de la incidencia:
Fecha y hora en que se produjo la incidencia:
Persona(s) a quien(es) se comunica**:**
Efectos que puede producir**:** (En caso de no subsanación o incluso independientemente de ella
Medidas correctoras aplicadas:
Recuperación de Datos :(A rellenar sólo si la incidencia es de este tipo) Procedimiento realizado: Datos restaurados: Datos grabados manualmente: Persona que ejecutó el proceso:
Firma del Responsable del fichero: Fdo _____
Persona que realiza la comunicación: Fdo.:_____