POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD POLITÉCNICA DE VALENCIA

1.- ÁMBITO DE APLICACIÓN

La presente ***Política General de Seguridad de la Información de la Universidad Politécnica de Valencia (UPV)*** es aplicable a todas las direcciones y gerencias, así como dependencias y campus, y tanto a sus empleados como alumnos, y también entidades y profesionales contratados bajo otras modalidades cuando en sus contratos se especifique.

2.- PROTECCIÓN DE LA INFORMACIÓN

En la UPV se reconoce expresamente la importancia de la información y de los sistemas de información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la entidad, o al menos suponer daños muy importantes si se produjera una pérdida irreversible de determinados datos. Además, por estar así establecido en la legislación española en lo que atañe a los datos de carácter personal, y en defensa de los intereses de los alumnos, profesores y empleados, proveedores, y otros posibles afectados.

Los accesos y usos de la información, por tanto, estarán en línea con lo que se indica en la presente política y en las normas, reglas, estándares y procedimientos de la UPV que se deriven de la misma.

Los empleados y alumnos (y usuarios en general) deberán conocer al menos un resumen de la política, normas, reglas, estándares y procedimientos, y deberán conocer de igual forma el ***Documento de Seguridad*** en lo que se refiere a datos de carácter personal en aquellas partes en las que les afecte.

En la práctica deberá haber separación de funciones y revisión independiente de las operaciones o transacciones realizadas cuando sea necesario, a partir de los registros, de quién ha hecho qué, cuándo y desde dónde.

En previsión de la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar la posible existencia de anomalías lo antes posible, se fomentará la difusión de información y se promoverá la formación en seguridad entre empleados y colaboradores.

Cada función sólo podrá realizar las tareas y acceder a los datos necesarios que se requieran para cumplir su cometido, es decir se considerará el principio del llamado **"mínimo privilegio"** para evitar accesos no autorizados.

Algunos de los riesgos frente a los que se deberán establecer controles adecuados y razonables, tanto preventivos, como de detección y correctivos son: errores y omisiones, sabotajes, vandalismo, espionaje industrial, trasgresión de la privacidad y tráfico de datos, acciones de otros agentes externos no autorizados, y cualesquiera otros que puedan influir en que la información no sea exacta, completa, en definitiva íntegra, o no esté disponible dentro del tiempo fijado.

Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y en general de cualquier activo de la UPV.

En el caso de baja del empleado o contratado deberá entregar llaves, tarjetas de acceso, material de UPV, equipos y cualquier tipo de información, y se eliminarán o bloquearán sus códigos de usuario de acceso a los sistemas; en el caso de baja disciplinaria, y si hubiera sospechas, se analizará si ha podido obtener copias, en papel o en otro soporte, de información clasificada, o haber introducido variaciones no autorizadas a programas de ordenador.

3.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Se designará internamente al **responsable propietario de cada fichero** o base de datos con datos de carácter personal, que será quien deberá promover el establecimiento de controles y medidas tendentes a proteger los datos bajo su responsabilidad.

4.- RESPONSABILIDADES

La responsabilidad de la seguridad de la información es de la Dirección del centro, departamento, área, instituto, servicio o unidad de la UPV correspondiente en cada caso, que pondrá los medios adecuados, lo que no obsta para que cada empleado o usuario asuma su parte de responsabilidad respecto a los medios que utiliza, según los puntos que se indican en esta política, en las normas que la desarrollan y en los procedimientos complementarios.

Quienes desempeñen funciones de **Seguridad de la Información** y otras de administración relacionadas, serán quienes administren la seguridad.

5.- SEGUIMIENTO Y CONTROL

Deberán realizarse periódicamente **evaluaciones de riesgos** y, en función de las debilidades detectadas, se determinará si es necesario elaborar planes de implantación o reforzamiento de controles.

La revisión de la seguridad, si bien ésta ha de ser una inquietud de todos, recaerá en funciones más relacionadas como aquellas de **control interno** en los centros y departamentos, **Seguridad de la Información** y sus corresponsales o colaboradores (por centros, por departamentos, por campus...), y **auditoría** (de sistemas de información) **interna**, sin perjuicio de que se pueda contratar auditoría de sistemas de información externa; la periodicidad de las revisiones en los sistemas críticos no debe ser superior a un año.

Esta política se matizará y desarrollará en un conjunto de normas así como a través de reglas, guías, estándares, y procedimientos, según sea necesario y avance la tecnología o se extienda la información a diferentes plataformas o centros.