Normativa de seguridad y privacidad “Consulta Modelo de Estado en la UPV”

1. SEGURIDAD EN EL USO DE MEDIOS INFORMÁTICOS.

1. No se almacenarán recursos que contengan datos personales en medios propios.
2. Se utilizarán las unidades o repositorios de Amazon Web Services para el almacenamiento de información.
3. A los efectos de esta normativa la información se considera confidencial o restringida.

2. CONTROLES DE ACCESO FÍSICO Y LÓGICO

1. La información se almacenará en medios, recursos o áreas sólo accesibles a personas autorizadas.
2. Cada usuario podrá acceder exclusivamente a los recursos y sistemas de información autorizados.
3. Los ordenadores y equipos vinculados al desarrollo del trabajo deberán disponer de un sistema de validación de usuario y contraseña.
4. En caso de ausencia del puesto, de trabajo en espacios que no excluyan a terceros debe procederse al bloqueo del puesto que en todo caso deberá producirse automáticamente tras 15 minutos de inactividad. En particular, cuando se trate de ámbitos de libre acceso el propio usuario deberá bloquear el acceso al abandonar el puesto.
5. En el diseño del puesto de trabajo se asegurará que la pantalla no resulte accesible o legible para terceros no autorizados.
6. Debe procederse a apagar el ordenador al finalizar el periodo de trabajo, así como evitar el uso del mismo por terceras personas.
7. Las contraseñas no deben ser almacenadas en ficheros legibles, macros, PCs sin control de acceso o ningún otro lugar donde puedan ser accedidas por personas sin autorización.
8. Es recomendable proceder al cambio de contraseñas cuando lo solicite el sistema, o en todo caso a iniciativa propia. Siempre deberá utilizar contraseñas seguras que incorporen ocho o más caracteres, mayúsculas, números o signos y que no deben ser palabras, nombres o conceptos.
9. Nunca deben facilitarse los datos de usuario y contraseña a ningún tercero.

3. USO, MANTENIMIENTO Y DESTRUCCIÓN DE DISPOSITIVOS O SOPORTES QUE CONTENGAN INFORMACIÓN PROTEGIDA

1. Los documentos deberán custodiarse en un sistema de almacenamiento seguro provisto de llave o clave que deberán ser custodiados debidamente por sus portadores.
2. No se debe dejar abandonada información en la impresora, fax o dispositivos similares, o desatendida en el puesto de trabajo.
3. Antes de abandonar salas comunes o permitir que alguien ajeno entre, se limpiarán adecuadamente las pizarras de las salas de reuniones o despachos que contuvieran información relacionada con el proyecto, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.
4. La impresión o fotocopia de documentos debe limitarse únicamente aquellos que sean estrictamente necesarios y preferiblemente a doble cara. Los documentos desechados, incluidas las fotocopias erróneas no podrán ser reutilizados cuando contengan datos personales o información confidencial o restringida debiéndose proceder a su inmediata destrucción.
5. En el caso de reutilización de documentos impresos el usuario comprobará previamente que éstos no contienen datos de carácter personal, comunicando la incidencia en caso contrario.
6. La destrucción de cualquier tipo de soporte automatizado (CD, DVD, Disco duro, Pen-drive, etc.) o manual (papel, cintas de vídeo, etc.) se realizará de forma que los datos que contenían no sean recuperables y en su caso a través de los procedimientos establecidos.
7. No podrán donarse soportes informáticos que contengan información protegida a ningún tercero sin que previamente se haya realizado un borrado completo del mismo.
8. Queda prohibido alojar información confidencial o restringida propia de la “Consulta Modelo de Estado en la UPV” en servidores externos en la “nube” no ofrecidos por la propia institución, en particular cuando se trate de datos personales contenidos en los sistemas de información.

4. RECURSOS INFORMÁTICOS

1. Todo usuario debe mantener actualizados los sistemas operativos, antivirus y cortafuegos (firewalls) de su equipo de trabajo mediante actualizaciones automáticas.

5. INCIDENCIAS DE SEGURIDAD

1. El usuario debe comunicar cualquier Incidencia de Seguridad que a su juicio ponga en peligro información protegida mediante notificación a consultamodelestatalaupv@evotebox.es.

6. PUBLICACIÓN.

1. La publicación de contenidos relacionados con la actividad se limitará a los documentos o informaciones de carácter público o en todo caso a aquellos para los se haya obtenido la debida autorización.
2. La información publicada debe garantizar los principios de proporcionalidad, autenticidad e integridad. En todo caso no se publicará información que pueda lesionar la dignidad de las personas participantes que en ningún caso podrán ser identificadas o identificables.
3. La información se publicará en todo caso anonimizada de modo irreversible.

Y, a tal efecto lo firma en Valencia a 3 de diciembre de 2018.

NIF	APELLIDOS, NOMBRE	FIRMA
	Perfil usuario/a:	
	E-mail para perfil Interventores/as:	
	ID Telegram para perfil Gestor/a usuarios/as:	