Registro de las actividades de tratamiento “Consulta Modelo de Estado en la UPV”

a) Nombre y los datos de contacto del responsable.

La Plataforma pel referèndum a la UPV está integrada por alumnado, profesorado y personal de administración y servicios de la Universitat Politècnica de València, que participan a título individual como miembros de la comunidad universitaria. Entendemos que la universidad tiene un papel fundamental en la sociedad y es por este motivo que debe de poner en el debate público todas aquellas cuestiones que ayuden a evolucionar y avanzar en el camino de la libertad y la igualdad. Atendiéndonos a nuestro principal valor, la democracia, creemos que es el momento de introducir en la esfera pública el debate entre monarquía y república en el estado español. Por lo tanto, nos constituimos como una plataforma que reclama al estado español la realización de un referéndum para abordar este debate largamente silenciado y que hoy en día no tiene solución. Por este motivo, nos unimos con otras plataformas de estudiantes del estado, y convocamos una consulta de opinión sobre el tipo de modelo de estado a España.

Nuestra dirección de correo electrónico es consultamodelestatalaupv@evotebox.es

b) Fines del tratamiento;

Se usan datos de identificación, cuenta de correo electrónico o NIF, para facilitar la participación en el *bot* "consultamodelestatalaUPV" que sirve para votar en el proceso “Consulta Modelo de Estado en la UPV”.

c) Categorías de interesados.

- Miembros de la comunidad universitaria de la Universitat Politècnica de València que cuenten con una dirección activa de correo electrónica bajo el dominio de esta institución.
- Personal de empresas prestadoras de servicios a la Universitat Politècnica de València.

d) Categorías de datos personales;

- Datos de identificación.
  - Usuario y cuenta de correo electrónico.
  - NIF.

e) Categorías de destinatarios.

No se ceden datos a ningún tercero.

f) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

En aplicación del artículo 32 sobre bloqueo de los datos de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales los datos se conservarán bloqueados durante tres años para verificar nuestra responsabilidad por los tratamientos. En ese periodo, no estarán

accesibles a ningún usuario y no será tratados, salvo por el administrador para facilitarlos si le fueran requeridos.

g) Medidas de seguridad.

- El sistema diferencia cuatro perfiles de usuario/a, a saber:

    1. Participante en la consulta.
    2. Interventores/as.
    3. Gestor/a usuarixs.
    4. Administrador/a.

- Para la encriptación de los datos personales de los usuarios y usuarias con el perfil "Participantes de la consulta" se utiliza la versión 3 el algoritmo de *Hash* Seguro (*SHA*, *Secure Hash Algorithm*). Según recoge la Wikipedia "SHA-3 usa una construcción de esponja, donde los datos son absorbidos (metafóricamente) y éstos son procesados para mostrar una salida de longitud deseada. En la fase de absorción, los bloques de datos pasan por una operación XOR y después son transformados usando una función de permutación, denominada *f*. SHA-3 además permite que contenga bits adicionales de información, esto protege al algoritmo contra ataques de extensión, a los que son susceptibles los estándares SHA-1, SHA-2 y MD5. Además la flexibilidad en sus parámetros lo hace útil para probar ataques criptoanalíticos y usarlo en aplicaciones ligeras."

- En relación a las medidas de seguridad relacionadas con el almacenamiento de la información generada durante la consulta, nuestro sistema está alojado en un proveedor de servicios con las garantías del Reglamento General de Protección de Datos (Amazon Web Services con tratamiento en Irlanda). Amazon Web Service dispone de la certificación ISO 27018 (https://d1.awsstatic.com/certifications/iso_27018_certification.pdf). La norma ISO 27018 (https://www.iso.org/standard/61498.html) es un código de conducta diseñado para proteger datos personales en la nube. Se basa en la norma sobre seguridad de la información 27002 y proporciona asesoramiento en materia de implementación en lo referente a los controles de la norma 27002 aplicables a la información personalmente identificable (PII). Además, proporciona un conjunto de controles adicionales y asesoramiento relacionado a fin de satisfacer los requisitos de protección de la información personalmente identificable en la nube no cubiertos por el conjunto de controles existentes de la norma ISO 27002.

- El sistema proporciona a los usuarias y usuarias con el perfil "Participantes de la consulta" un mecanismo de autentificación para acceder a la consulta que funciona de la siguiente forma:

  Para participar en la consulta se utiliza la dirección de correo electrónico de la UPV para comprobar que se trata de un miembro de la comunidad universitaria y que se cumple el principio "una persona un voto". Para ello, se envía un número de cuatro cifras que debe introducirse en el *bot*. Una vez validado el número el sistema plantea al usuario o usuaria la primera pregunta ("¿Estás a favor de cambiar la monarquía por una república como forma de Estado?") y le ofrece tres posibles respuestas ("Sí", "No", "Abstención"). En caso de

contestar afirmativamente, el *bot* le plantea una segunda pregunta (“¿Estás a favor de abrir procesos constituyentes para decidir qué tipo de república?”) ofreciendo las mismas opciones de respuesta. Antes de proceder a registrar las respuestas introducidas el *bot* le al usuario o usuaria que las valides. A partir de ahí, el sistema almacena de forma encriptada la dirección de correo para proteger los datos personales en la nube y almacena las respuestas separadamente para garantizar el voto anónimo.

Para aquellas personas que trabajan en la UPV y no son personal de la universidad se ha habilitado un mecanismo para que puedan participar de la consulta en igualdad de condiciones que el resto de miembros de la comunidad universitaria. Para ello, deben proporcionar su NIF y una cuenta personal de correo electrónico. A partir de ahí, el procedimiento de voto es el mismo que para el resto de miembros de la comunidad universitaria. Tanto el NIF como la dirección de correo electrónico se almacenan de forma encriptada y las respuestas se registran de forma anónima.

- El sistema proporciona a los usuarias y usuarias con el perifl “Gestores/as de usuarios/as” un mecanismo de autentificación automático basado en el identifidor de usuario único proporcionado por Telegram. De esta forma, únicamente podrán acceder con este perfil aquellos usuarios y usuarias cuyos identificadores de Telegram hayan sido dados de alta en el sistema por los usuarios o usuarias con perfil “Administrador/a”.
- El sistema proporciona a los usuarias y usuarias con el perifl “Administrador/a” un mecanismo de autentificación Multi-Factor Authentication (MFA, autenticación multifactor) para acceder a los servicios de AWS. Este sistema añade una capa adicional de protección además del nombre de usuario y la contraseña. Mediante este sistema cuando un usuario o usuaria inicia sesión en un sitio web de AWS se solicita que indique el nombre de usuario o usuaria y la contraseña, así como una respuesta de autenticación del dispositivo MFA de AWS. Al combinar ambos factores, se mejora la seguridad de la configuración y los recursos de su cuenta de AWS.