**Especificación de Atributos de Calidad**

**Restricciones en la clave del registro de un cliente web**

**Categoría**: Seguridad.

**Fuente del estímulo**: Cliente web accede a la página y no posee una cuenta.

**Estímulo**: Acceso al registro del sistema para crear una cuenta.

**Artefacto**: Sistema de Registro del Sistema y base de datos de los usuarios.

**Ambiente o contexto**: Cliente-web trata de crear una cuenta a través de “Register” en el sistema.

**Respuesta**:

1. Los clientes-web podrán definir su clave
2. La clave se encriptará para toda transacción.
3. La clave se almacenará encriptada en la base de datos de usuarios.

**Medición de la respuesta**:

1. Clientes podrán tener un campo para insertar su clave, y el campo manejará reglas definidas para la aceptación de los datos.
2. Usar un estándar de encriptación de datos, donde el valor reemplazado sea largo, difícil de descifrar y tan aleatorio como sea posible.
3. La Base de Datos se relacionará con el componente de encriptación, para que tanto en la página como en la base de datos las claves sean indescifrables.

**Este escenario se logrará mediante las siguientes tácticas**:

1. El campo para introducir la clave, no permitirá dejar el campo como vacío, deberá ser obligatorio, además la clave deberá estar en un rango de entre 6 y 40 caracteres.

Al introducir la clave, esta aparecerá oculta, gracias a la utilización de las convenciones de cakephp al esperar una entrada “password” además se deberá confirmar dicha clave en un campo extra en el registro, donde ambos campos deberán validarse mediante una función “checking” definida en el modelo de usuarios.

1. Antes de guardar cualquier clave en la base de datos, se encriptará dicha clave, utilizando la clase “BlowfishPasswordHasher” disponible en CakePHP que utiliza bcrypt, el cuál es un algoritmo de hashing que se provee “salts”, información aleatoria adicional para ponerla en conjunto con la clave ingresada.
2. Verificar que la clave y el “salt” se concatenen y sea procesados por la función hash del algoritmo en la base de datos.