Especificación de Atributos de Calidad
Encriptación de la clave de los usuarios

Categoría: Seguridad.

Fuente del estímulo: El usuario provee su clave al momento de registrarse.

Estímulo: Escribe su clave y presiona “Submit”.

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

Ambiente o contexto: Usuario malintencionado trata de acceder a la información de la clave del usuario.

Respuesta: La clave se almacenará encriptada en la base de datos de usuarios.

Medición de la respuesta:

1. Usar un estándar de encriptación de datos, donde el valor reemplazado sea largo, difícil de descifrar y tan aleatorio como sea posible.

2. 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. 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.