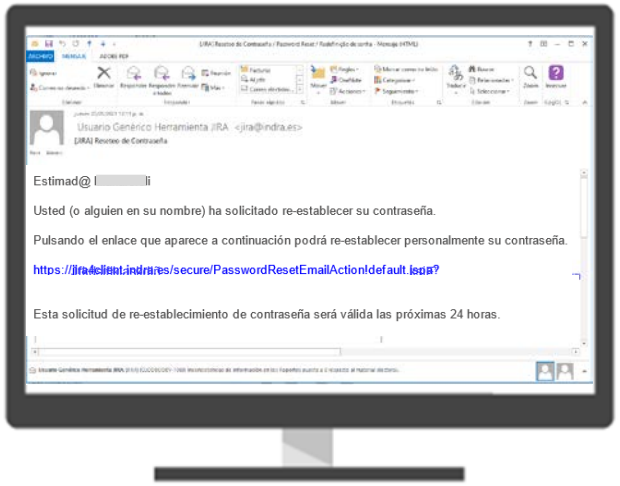
¿El software contempla elementos para asegurar la autenticidad de los usuarios?

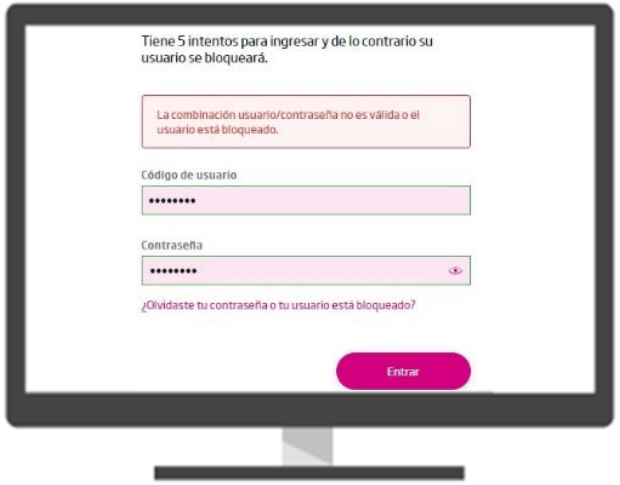
Enlace de única ocasión



Los enlaces de única ocasión sirven para robustecer la autenticidad de los usuarios, al proporcionarles normalmente mediante correo electrónico un enlace donde pueda activar una cuenta de usuario o cambiar su contraseña, entre otras opciones. Para su evaluación se recomiendan los siguientes casos de prueba:

- ❏ Ingresar a la URL y no realizar el movimiento, o dejarlo inconcluso. El sistema debe permitir llevar a cabo la acción posteriormente.
- ❏ Probar la URL con 2 ó 3 usuarios al mismo tiempo, asegurar que sólo se ocupe en una ocasión y a los demás usuarios impedirles guardar el movimiento.
- ❏ Uso de una URL no utilizada durante el tiempo establecido.
- ❏ Uso de una URL previamente utilizada.
- ❏ Realizar el flujo de información omitiendo el uso de la URL.

Bloqueo de la cuenta de usuario después de determinado número de intentos de accesos fallidos



Un elemento de seguridad para fortalecer el acceso a usuarios autorizados es mediante el bloqueo de la cuenta de usuario al recibir cierto número de intentos fallidos. Para su revisión se sugieren los siguientes casos de prueba:

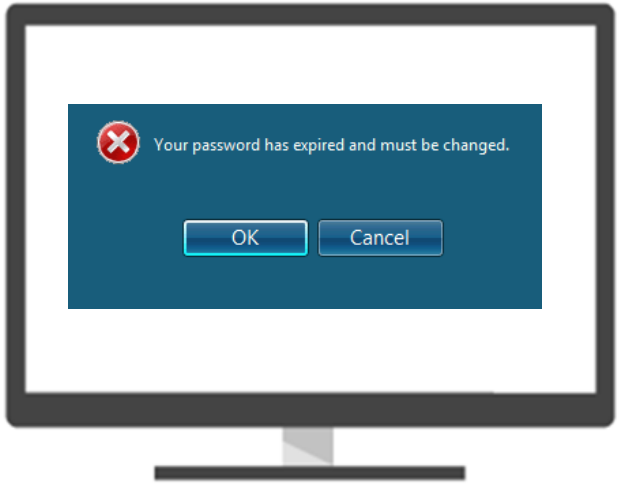
- ❏ El sistema contempla el bloqueo de usuarios por mal uso de la cuenta o accesos fallidos.
- ❏ Ingresar el número de intentos fallidos (de 3 a 5) para bloquear la cuenta de usuario. El sistema debe bloquear la cuenta, notificar al usuario, y no debe permitir el acceso al sistema aún ingresando los datos correctos.
- ❏ Bloquear la cuenta de usuario, desbloquearla e intentar un ingreso fallido. El sistema debió haber reiniciado el número de intentos fallidos por lo cual la cuenta debe estar desbloqueada.
- ❏ Ingresar los elementos de acceso correctos en el último intento para ser bloqueado. El sistema debe permitir la autenticación y reiniciar el número de intentos fallidos.
- ❏ El sistema debe tener un mecanismo de desbloqueo de las cuentas de usuario.

Tiempo de expiración de una sesión

Otro elemento para asegurar la autenticidad de los usuarios es, el cierre de la sesión de los usuarios después de un tiempo de inactividad, para evitar que una persona ajena pueda usurpar momentáneamente al usuario, realizando movimientos en el sistema. Para la revisión de este elemento se recomiendan los siguientes caso de prueba:

- El sistema considera la expiración de una sesión por tiempo de inactividad.
- Autenticarse y dejar abierta la sesión sin realizar ningún movimiento (generalmente el tiempo de inactividad va de 15 a 30 minutos), trabajando en otro navegador o aplicación. El sistema debe notificar el cierre de sesión.
- Autenticarse en el sistema y dejar abierta la sesión sin realizar ningún movimiento, haciendo uso de otra pestaña del mismo navegador. El sistema debe contabilizar el tiempo de inactividad en el sistema y cerrar la sesión.
- En caso de presentar funcionalidad para reanudar la sesión, el sistema reinicia el tiempo de expiración de sesión.

Expiración de la contraseña de una cuenta de usuario



Con la finalidad de fortalecer la autenticidad de los usuarios y disminuir el riesgo de descubrir la contraseña de alguno, se recomienda que las contraseñas tengan vencimiento y se modifiquen periódicamente para que ningún otro usuario malintencionado obtenga acceso al sistema. Para evaluar este elemento se sugiere revisar:

- El sistema contempla la caducidad en la contraseña de una cuenta de usuario.
- Al caducar la contraseña de la cuenta de usuario el sistema impide el acceso al sistema.
- El sistema permite cambiar la contraseña previo a caducarse.
- El sistema permite cambiar la contraseña una vez caducada, permitiendo nuevamente el acceso al sistema.
- La contraseña no puede repetirse al menos en las últimas 3 actualizaciones.