

¿El sistema contempla elementos de seguridad en la autenticación?



Los elementos de seguridad son utilizados para confirmar la identidad del usuario, así como para determinar cuando el usuario es un humano o un programa automático. Los elementos biométricos y doble factor de autenticación se utilizan como complemento o en lugar de una contraseña, actúan como una llave electrónica para acceder al sistema.



Algunos de los elementos para verificar que se trata de un humano son: agudeza visual, resolver operaciones matemáticas, identificar imágenes, pequeños juegos y no soy un robot.

Casos de prueba sugeridos:

- ☐ No seleccionar la opción "No soy un robot".
- ☐ No ingresar lo que se solicita (cadena, valor, selección).
- ☐ Ingresar lo solicitado con información diferente.



Para fortalecer el acceso autorizado de los usuarios, cuando se haga uso de doble factor de autenticación, certificados, tokens, elementos biométricos o firmas electrónicas, se sugiere probar:

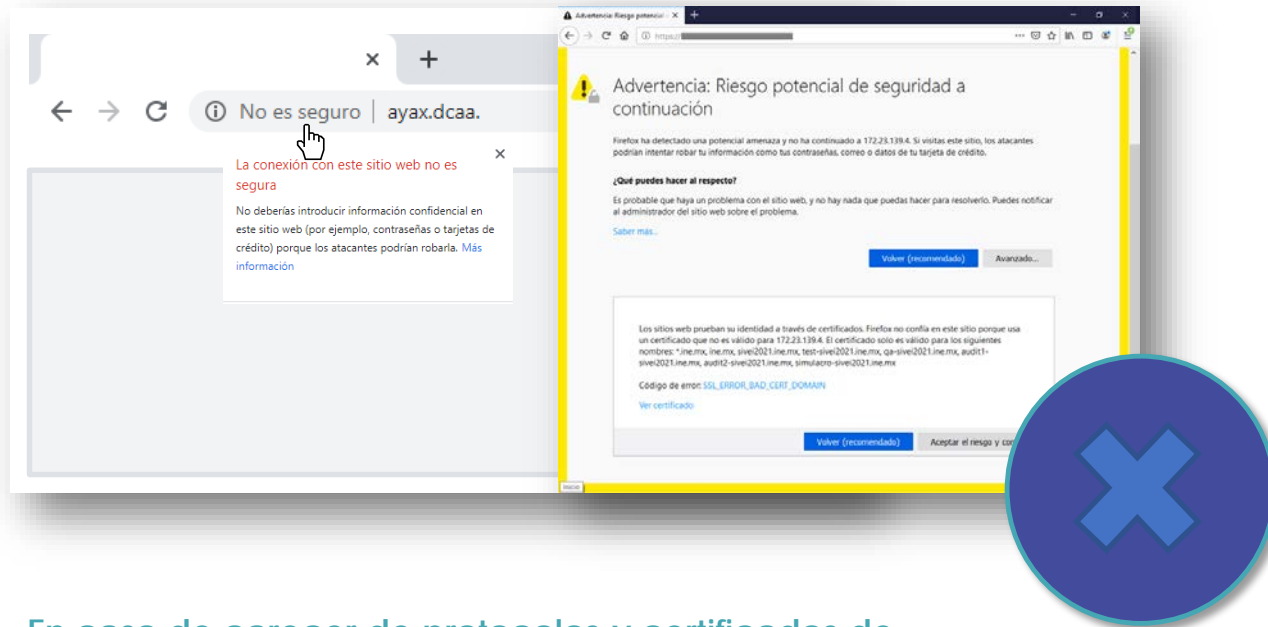
Casos de prueba sugeridos:

- ☐ No ingresarlo.
- ☐ Ingresar el elemento de autenticación de otro usuario.
- ☐ Ingresar el elemento de autenticación caducado.
- ☐ Ingresar el elemento de autenticación dañado.
- ☐ Ingresar lo solicitado con información diferente / inexistente.



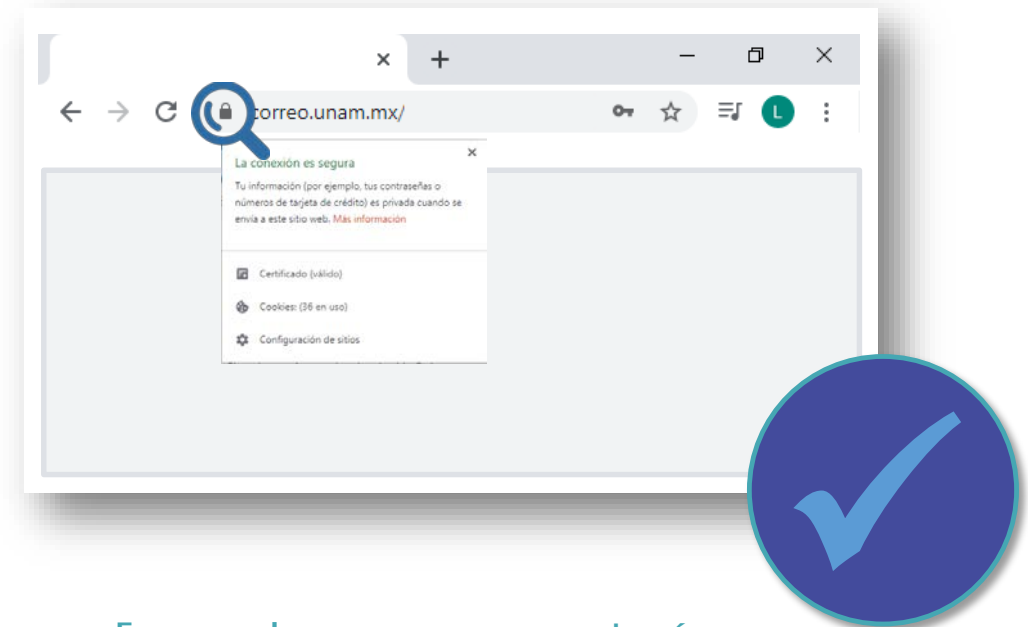
Otro de los elementos a comprobar es si el sistema en web contempla el uso de páginas seguras, donde se sugiere que en cualquier navegador se despliegue la URL y se consulte el estado de seguridad, el cual se encuentra previo a la dirección web.

Es importante mencionar que la prueba se tiene que hacer en el ambiente de producción, debido a que la mayoría de las veces los ambientes de pruebas carecen de esta seguridad, lo cual es adecuado.



En caso de carecer de protocolos y certificados de seguridad, mostrará una advertencia como las siguientes:

- ❑ El sitio web al que vas a acceder contiene software malicioso / programas dañinos.
- ❑ Advertencia: Riesgo potencial de seguridad.
- ❑ Sitio web sospechoso.
- ❑ Esta página está intentando cargar scripts de fuentes no autorizadas.



En caso de ser seguro se mostrará una imagen de un candado cerrado, indicando que cuenta con los protocolos y certificados de seguridad.

Departamento de Aseguramiento de Calidad de Proyectos de Software
DCV - DGTIC, UNAM

