****

***Dirección Nacional de Desarrollo del Servicio de Rentas Internas***

**Informe Justificativo**

**Credenciales de Usuarios**

**cgad070313**

Contenido

[1. Descripción 1](#_Toc388525367)

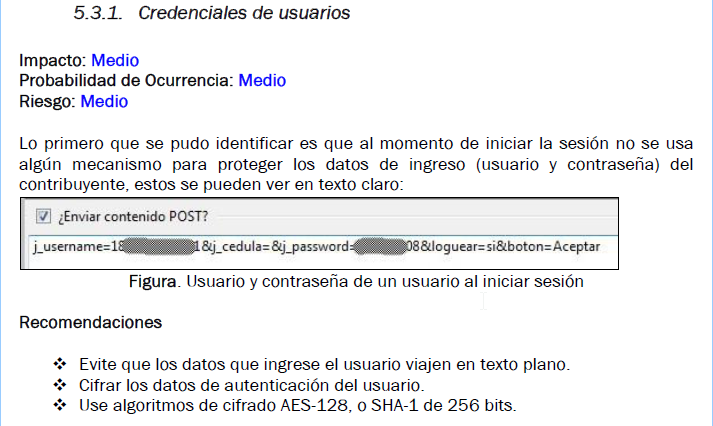
[2. Análisis: 1](#_Toc388525368)

[3. Conclusiones: 2](#_Toc388525369)

[4. Justificativo: 3](#_Toc388525370)

# Descripción

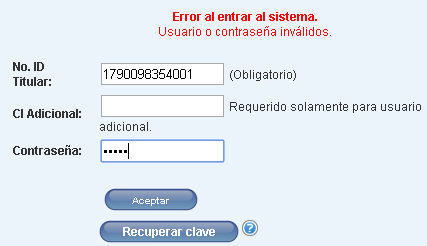
En el informe de pruebas extensas provisto por la empresa Seltika, se muestra la siguiente alerta de seguridad:



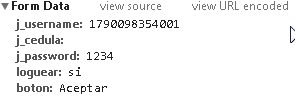
# Análisis:

Mediante la réplica del error se pudo comprobar lo siguiente:

* El error se reproduce en los siguiente escenario:
  + Se instala las herramientas de desarrollador web disponibles tanto para browsers como Firefox y Chrome.
  + Se procede a activar la consola de estas herramientas.
  + El usuario ingresa a la url <https://declaraciones.sri.gob.ec/tuportal-internet/> y procede a autenticarse en el sistema. Fig. 1
  + Podemos visualizar los valores que se transportan en texto plano. Fig. 2



**Fig. 1**



**Fig. 2**

* Este error fue detectado en el proyecto en la página llamada login.jsp en el formulario de datos de inicio de sesión y donde se utiliza **j\_security\_check**.

# Conclusiones:

Mediante la evaluación forma y la tecnología con la que se implementó este inicio de sesión se determinó lo siguiente:

* Se están utilizando los parámetros necesarios para garantizar el nivel muy seguro de transporte de los datos mediante la conexión con protocolo seguro HTTPS .
* El formulario se envía mediante método POST.
* Los datos en texto plano pueden ser visto mediante el proceso de replicación del error descrito anteriormente y del lado del cliente (browser).
* Se sometió a la misma prueba otros formularios dando el mismo resultado, dado que la información es la que permanece del lado del usuario final o cliente.

# Justificativo:

La presente alerta de seguridad atañe exclusivamente al lado del cliente lo cual se vuelve muy difícil de controlar por estar del lado del browser, más sin embargo la información al momento de transportarse por la red se encuentra protegida y el ambiente del lado del servidor no se ha comprometido.

Algunas posibles soluciones de encriptación del lado del cliente mediante javascript fueron evaluadas, más sin embargo representan una medida de seguridad muy superficial que no alcanza a solventar el tema por completo.