

## Informe Certificación de Seguridad

SSO Web 1.0.0.0



*05 de marzo de 2015*

## Hoja de Control del Documento

Información del Documento			
<b>Título</b>	Informe Certificación de Seguridad		
<b>Asunto</b>	SSO Web 1.0.0.0		
<b>Nombre del fichero</b>	SSO Web 1.0.0.0_CAL_Informe Certificación de Seguridad_v01r00.doc		
<b>Versión</b>	v01r00		
<b>Elaborado por</b>	Centro de Calidad Integral	<b>Fecha Elaboración</b>	05/03/2015
<b>Aprobado por</b>		<b>Fecha Aprobación</b>	
<b>Confidencialidad</b>			

Control de Versiones			
Versión	Descripción de los cambios	Elaborado por	Fecha Elaboración
01r00	Elaboración inicial del documento	Centro de Calidad Integral	05/03/2015

Lista de Distribución	
Nombre Apellidos	Cargo / Función
Juan Sebastián Ojeda Pérez	Jefe de Servicio de Coordinación y Desarrollo de Sistemas Horizontales
Javier García de Bringas	Jefe de Servicio Planificación Estratégica
Antonio Blanco Morales	Jefe de Gabinete de Desarrollo de Infraestructura SW
Gabriel Medel Valpuesta	Jefe de Gabinete Administración Electrónica Tributaria
Francisco Rodríguez Corredor	Responsable de proyectos
Rosario Ochoa Zalduendo	Jefe de Proyecto Centro de Calidad Integral
Esther Fraile Amodeo	Responsable de Calidad y Certificación
Javier Ruiz Hidalgo	Analista de Pruebas



## ÍNDICE

1.	RESUMEN EJECUTIVO .....	4
1.1.	Objetivos y Alcance .....	4
1.1.	Resultado.....	4
1.2.	Conclusiones.....	4
1.3.	Incidencias y Problemas.....	4
2.	ALCANCE Y CARACTERÍSTICAS DE LA CERTIFICACIÓN .....	5
3.	RESULTADOS GLOBALES .....	6
4.	DEFECTOS ENCONTRADOS EN LAS VERIFICACIONES APLICADAS.....	7
5.	ANEXO .....	8
5.1.	Normativa Aplicada.....	8
5.2.	Detalle de Resultados.....	8
5.2.1.	Verificaciones Seguridad .....	8



## 1. RESUMEN EJECUTIVO

### 1.1. Objetivos y Alcance

El Servicio tiene como misión detectar posibles vulnerabilidades del Sistema, con el objeto de minimizar el riesgo de materialización de amenazas y proponer salvaguardas.

### 1.1. Resultado

A continuación, se muestra el resultado de la ejecución de la Certificación de Seguridad, respecto a los niveles de calidad establecidos por la DGPD:


Resultado Global		
Nivel Alcanzado	Es vulnerable a XSS, Inyección, CSRF, Fijación de Sesión o fuerza bruta	
Nivel Objetivo	No se deben presentar defectos	
Resultado Final	Nivel de Calidad no alcanzado, quedando muy lejos del Objetivo	

Tabla 1 – Resultado de la ejecución del Servicio

### 1.2. Conclusiones

Se ha detectado que el sistema es vulnerable a ataques de fuerza bruta. Al tratarse de un producto, el sistema pasa con soltura el resto de verificaciones ejecutadas.

La importancia del único defecto detectado hace que la calidad del sistema se quede lejos del nivel marcado como objetivo.

### 1.3. Evolución respecto a la ejecución anterior

Dado que esta es la primera versión que se realiza de este sistema, no podemos hablar de evolución respecto a ejecuciones anteriores.

### 1.4. Incidencias y Problemas

No se han producido incidencias o problemas durante la realización de la certificación.



## 2. ALCANCE Y CARACTERÍSTICAS DE LA CERTIFICACIÓN

El Servicio de Certificación de Seguridad se define tomando como marcos de referencia el Esquema Nacional de Seguridad y OWASP. Según las características del Sistema y su uso, el Centro de Calidad Integral establece unos requisitos mínimos que quedan recogidos en el conjunto de vulnerabilidades a estudiar.

Este Servicio pone de manifiesto cuáles son los activos de información del Sistema así como las amenazas más Altas que se plantean. La detección de vulnerabilidades se realiza en base a herramientas automatizadas y verificaciones manuales realizadas por expertos en la materia, que permiten analizar el comportamiento del Sistema.



### 3. RESULTADOS GLOBALES

El resultado obtenido se detalla a continuación, indicando el número de vulnerabilidades encontradas en la siguiente tabla según su severidad:

ID	Descripción	Severidad
SEG-1	La aplicación es vulnerable a ataques de fuerza bruta	Media

Tabla 2 – Resumen Defectos Encontrados Organizados por Severidad

Resumen de defectos encontrados según el nivel de severidad, comparadas con nivel de calidad deseado:

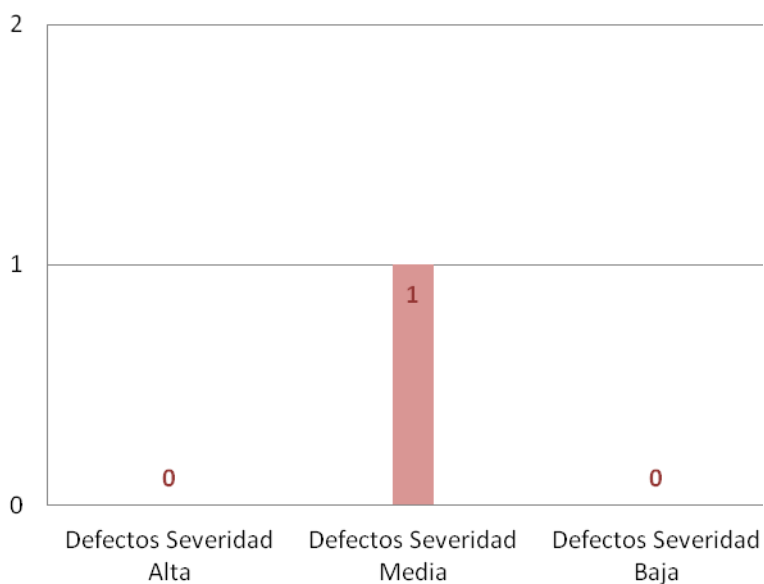


Gráfico 1 - Distribución de Defectos



**4. DEFECTOS ENCONTRADOS EN LAS VERIFICACIONES APLICADAS**

Defectos				
ID	Descripción del Indicador	Descripción del Defecto	Severidad	Referencia Anexa
SEG-1	La aplicación es vulnerable a ataques de fuerza bruta	El formulario de autenticación de SSO Web es vulnerable a ataques basados en fuerza bruta, ya que se pueden realizar más de 30 intentos de inicio de sesión con diferentes usuarios y contraseñas sin que se bloquee el acceso.	Media	

Tabla 3 –Defectos



## 5. ANEXO

## 5.1. Normativa Aplicada

El presente Servicio tiene como misión detectar posibles vulnerabilidades de la aplicación, con el objeto de minimizar el riesgo de materialización de amenazas y proponer salvaguardas. El servicio se define tomando como marcos de referencia el Esquema Nacional de Seguridad y OWASP.

El Servicio se ha adecuado al Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero) para sustentarlo dentro de un marco normativo de nivel nacional que ha supuesto la incorporación de nuevas verificaciones a exigir y la adopción de un lenguaje común con el que facilitar la obtención de sinergias.

## 5.2. Detalle de Resultados

El resultado obtenido para cada uno de los criterios sobre los que se ha ejecutado el servicio, se corresponde con:

- ☒ Criterio Superado
- ☐ Criterio No Superado
- ☐ Recomendación
- N/A Verificación no ejecutada

A continuación, se muestran detalladamente las verificaciones ejecutadas junto a su correspondiente resultado:

## 5.2.1. Verificaciones Seguridad

Verificaciones			
Identificador	Descripción	Resultado	Severidad
SEG-1	La aplicación es vulnerable a ataques de fuerza bruta	<input type="checkbox"/>	Media
SEG-2	Existe un control en la aplicación para evitar el acceso tras un tiempo inactivo.	<input checked="" type="checkbox"/>	Media
SEG-3	La desconexión de la sesión debe ser controlada desde la aplicación tras un tiempo de inactividad.	<input checked="" type="checkbox"/>	Baja
SEG-4	La aplicación tiene implementado funcionalidad para salir de la misma y evitar robo de identidad.	<input checked="" type="checkbox"/>	Media
SEG-5	Identificación de escenarios de denegación de servicio por bloqueo de cuentas de usuarios tras un número determinado de intentos de acceso fallidos.	<input checked="" type="checkbox"/>	Baja
SEG-6	La aplicación es vulnerable a ataques de Cross-Site Scripting (XSS)	N/A	Alta
SEG-7	La aplicación es vulnerable a ataques de inyección SQL	N/A	Alta
SEG-8	La inyección LDAP es evitada por la aplicación	<input checked="" type="checkbox"/>	Alta
SEG-9	La inyección XML es evitada por la aplicación.	N/A	Media
SEG-10	Verificar que la aplicación no permite inyección de comandos en el sistema operativo.	<input checked="" type="checkbox"/>	Media





Verificaciones			
Identificador	Descripción	Resultado	Severidad
SEG-13	Verificar que en la operación de cambio de contraseña se solicita el valor antiguo del mismo.	N/A	Media
SEG-14	La aplicación no utiliza un protocolo seguro para enviar la información crítica.	■	Alta
SEG-16	Comprobar que la información sensible es tratada sin cifrar solo en las ocasiones en la que es imprescindible descriptarla.	N/A	Baja
SEG-17	Protección insuficiente de la capa de transporte	■	Alta
SEG-18	La aplicación contiene información inapropiada en la url	■	Baja
SEG-19	No deben mostrarse en la URL parámetros cuyo nombre pueda indicar la información que contienen.	■	Baja
SEG-20	Las referencias cruzadas de páginas no deben contener información de direcciones IP físicas.	■	Baja
SEG-21	Comprobar que no se pueden realizar ataques por fijación de sesión, ni se revela el o los parámetros que identifican la sesión en la URL.	■	Alta
SEG-22	Comprobar que el o los parámetros que identifican la sesión no se generan mediante algoritmos predecibles.	■	Media
SEG-23	Verificar que no existe un inapropiado manejo de la información y de errores que puedan ayudar a aumentar el riesgo de otras vulnerabilidades.	■	Baja
SEG-24	Verificar que no se utilizan cuentas y usuarios predeterminados o predecibles.	N/A	Baja
SEG-25	La aplicación permite el escalado de privilegios en partes concretas	N/A	Alta
SEG-26	Verificar que se registra los accesos de los usuarios al sistema.	N/A	Baja
SEG-27	Comprobar que no se puede realizar una ejecución maliciosa de archivos en el lado del servidor pudiéndose perder el control total sobre la máquina.	N/A	Alta
SEG-29	La aplicación carece de token por lo que es vulnerable a ataques de CSRF	N/A	Alta
SEG-30	Verificar que no se pueden realizar ataques de manipulación de "proxys" o "caches" (por ejemplo mediante http response splitting).	N/A	Media
SEG-31	La aplicación no restringe el acceso a ciertas URL's	N/A	Media
SEG-32	Verificar que no se puede acceder a la información mediante protocolos con niveles de seguridad diferentes (por ejemplo http y https).	■	Media
SEG-36	Verificar que no se utilizan campos HTML ocultos que almacenan información sensible sin establecer mecanismos de seguridad.	■	Media



Verificaciones			
Identificador	Descripción	Resultado	Severidad
SEG-37	Verificar que no es posible evitar los controles de seguridad que evalúan si el usuario no es un proceso automático (captcha, etc.).	N/A	Baja
SEG-39	Verificación de las vulnerabilidades públicas existentes para los productos utilizados o integrados en la aplicación.	■	Alta
SEG-40	Verificación de vulnerabilidades específicas del aplicativo auditado, como puede ser por ejemplo en un servicio de webmail, no poder enviar mensajes suplantando la identidad de otro usuario.	■	Alta

Tabla 4 –Verificaciones

