JUNTA DE ANDALUCIA

CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

# Ventanilla Electrónica

## Auditoría de Seguridad

Versión: v01r00

Fecha: 26/05/2015

# HOJA DE CONTROL

| | | | |
|---|---|---|---|
| **Título** | Auditoría de Seguridad | | |
| **Entregable** | Auditoría de Seguridad | | |
| **Nombre del Fichero** | VEA230E_OTR_Auditoria_de_Seguridad_v01r00.doc | | |
| **Autor** | UTE | | |
| **Versión/Edición** | v01r00 | **Fecha Versión** | 26/05/2015 |
| **Aprobado por** | - | **Fecha Aprobación** | DD/MM/AAAA |
| | | **Nº Total Páginas** | 13 |

## REGISTRO DE CAMBIOS

| Versión | Causa del Cambio | Responsable del Cambio | Área | Fecha del Cambio |
|---|---|---|---|---|
| v01r00 | Versión inicial | everis | - | 26/05/201 |
| - | - | - | - | - |

## CONTROL DE DISTRIBUCIÓN

| Nombre y Apellidos | Cargo | Área | Nº Copias |
|---|---|---|---|
| Manuel Perera Domínguez | Jefe de Servicio | Servicio de Coordinación de Administración Electrónica | 1 |
| Francisco González Guillén | Director de proyecto | Servicio de Coordinación de Administración Electrónica | 1 |
| Francisco Mesa Villalba | Director de proyecto | Servicio de Coordinación de Administración Electrónica | 1 |
| Pedro José Casanova Luis | Jefe de Proyecto | UTE | 1 |

# ÍNDICE

# 1 INTRODUCCIÓN

La finalidad del presente documento es realizar una auditoría de seguridad del componente Ventanilla Electrónica, detectando las posibles vulnerabilidades del sistema con el objeto de minimizar el riesgo de materialización de amenazas a las que está expuesto y proponer las salvaguardas necesarias. Todo ello para poder garantizar un nivel de seguridad adecuado que permita aseverar que VEA es resistente a los principales ataques de seguridad conocidos hasta el momento y no supone un agujero de seguridad para los sistemas de información de los organismos en los que se despliegue la aplicación.

Para la verificación de la seguridad de la aplicación se ha aplicado una lista de indicadores obtenidos a partir de los definidos por la OWASP (Open Web Application Security Project), para garantizar la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos a los que se enfrentan las organizaciones. La lista de los principales riesgos identificados por la organización, se enumeran a continuación:

- Inyección
- Secuencia de comandos de sitios cruzados (XSS)
- Perdida de autenticación y gestión de sesiones
- Referencia directa insegura a objetos
- Falsificación de peticiones en sitios cruzados (CSRF)
- Defectuosa configuración de seguridad
- Almacenamiento criptográfico inseguro
- Falla de restricción de acceso URL
- Comunicaciones inseguras
- Redirecciones y reenvíos no validados
- Vulnerabilidades a través de servicios web
- Ficheros adjuntos
- Fuga de información

Además de estos riesgos, se han incluido los indicadores que pueden ser verificados con el conjunto de herramientas utilizadas para el análisis del nivel de seguridad de aplicaciones:

- W3af
- Grendel-Scan
- Paros proxy
- WebScarab
- Firefox-Firebug

Con las herramientas mencionadas se han aplicado test de intrusión, verificaciones semi-manuales, escáneres de detección prematura de vulnerabilidades, y análisis a nivel de protocolo http, detectándose y obteniéndose un estudio completo de las vulnerabilidades existentes en la aplicación. Para ello, las tareas han sido realizadas accediendo a la aplicación en los términos adecuados, y procediendo con su observación, interacción y navegación de la misma.

Las pruebas se han realizado sobre la aplicación desplegada en el entorno de certificación de la empresa everis, correspondiente a la versión en fase de liberación por parte de la Consejería de Hacienda y Administración Pública.

# 2 RESULTADO DE LA REVISIÓN

| Indicadores de revisión de seguridad | | | | |
|---|---|---|---|---|
| **Código** | **Descripción del Indicador** | **¿Cumple?** | **Observaciones** | **Severidad** |
| **SEG-01** | El listado de directorios de la aplicación no puede ser visible por URL | ☒ | | Alta |
| **SEG-02** | No deben mostrarse en la URL parámetros. | ☒ | | Media |
| **SEG-03** | No deben mostrarse en la URL parámetros cuyo nombre pueda indicar la información que contienen | ☒ | | Alta |
| **SEG-04** | En el caso de que haya referencia a URLs externas o a ficheros del propio sistema se deben validar. | ☒ | | Alta |
| **SEG-05** | La aplicación no debe mostrar información referente a la BD en los errores producidos (Errores ORA). | ☒ | | Media |
| **SEG-06** | La aplicación no debería mostrar información referente al cliente en los errores producidos (ERROR -jsessionid bloqueado). | ☒ | | Media |
| **SEG-07** | El acceso a aplicaciones internas debe estar limitado a ubicaciones internas de la Junta de Andalucía | ☒ | La aplicación se puede configurar para que se integre con cualquier otra aplicación sin distinción de la ubicación en la que se encuentre | Media |
| **SEG-08** | La autenticación en la aplicación debe iniciarse desde una página cifrada | ☒ | La autenticación de la aplicación se realiza desde una página que utiliza un protocolo no seguro (http). Aunque la aplicación se encuentra en un entorno de prueba, y por tanto puede justificarse que en este entorno no es necesario utilizar el protocolo https. | Alta |
| **SEG-09** | Las páginas de la aplicación deberían disponer de un enlace para cerrar la sesión activa en cualquier momento. | ☒ | | Media |

| Indicadores de revisión de seguridad | | | | |
|---|---|---|---|---|
| **Código** | **Descripción del Indicador** | **¿Cumple?** | **Observaciones** | **Severidad** |
| **SEG-10** | La aplicación debe controlar el evento de cierre de la ventana para cerrar la sesión activa. | ☒ | | Media |
| **SEG-11** | Debería estar establecido un periodo determinado de tiempo que cierre la sesión inactiva. | ☒ | Este periodo determinado de tiempo se configura en los web.xml de la aplicación. | Media |
| **SEG-12** | Se debe controlar el procedimiento de acceso a la aplicación, de forma que un número de accesos incorrectos bloquee el acceso en la sesión. | ☒ | El procedimiento de acceso conlleva la selección de un certificado digital. | Media |
| **SEG-13** | En caso de aplicaciones cuyo acceso se realiza mediante usuario/password, en el cambio de password se debe solicitar el valor antiguo del mismo. | ☒ | El acceso se realiza mediante certificado digital. | Baja |
| **SEG-14** | Los datos que por requisitos de la aplicación son almacenados en el cliente, como las cookies, deben ser cifrados o firmados. | ☒ | La aplicación no envía ningún dato que deba ser almacenado en el cliente. | Baja |
| **SEG-15** | EL acceso a una aplicación a través de una URL que dirige a una página interna, debe redirigir a un punto de entrada en el que el usuario deba autenticarse para poder ser dirigido a la página referenciada inicialmente. | ☒ | Para todas las páginas que requieran de la autenticación del ciudadano se comprueba que dicho ciudadano esté logado en el sistema, de no ser así se redirige automáticamente a una página de autenticación. | Alta |
| **SEG-16** | No se deben utilizar campos HTML ocultos para almacenar información sensible sin establecer un mecanismo de seguridad. | ☒ | | Baja |
| **SEG-17** | Debe controlarse el acceso a cualquier punto de la aplicación sin que haya realizado la validación adecuada. | ☒ | Se controla en todo momento que el ciudadano esté debidamente logado en el sistema en aquellas páginas que así lo requieran. | Alta |
| **SEG-18** | No se deben almacenar archivos obsoletos en directorios de la aplicación dentro del servidor de aplicaciones. | ☒ | | Baja |
| **SEG-19** | No se debe mostrar información referente al servidor en los errores producidos. | ☒ | | Media |
| **SEG-20** | Las referencias entre páginas no deben ser codificadas mediante direcciones IP físicas. | ☒ | | Baja |

| Indicadores de revisión de seguridad | | | | |
|---|---|---|---|---|
| **Código** | **Descripción del Indicador** | **¿Cumple?** | **Observaciones** | **Severidad** |
| **SEG-21** | En los mensajes lanzados al usuario no deberían mostrarse IPs físicas. | ☒ | | Media |
| **SEG-22** | En los errores del servidor no se deben mostrar al usuario trazas del error, sino que se debe mostrar información de error genérica. | ☒ | | Media |
| **SEG-23** | No se deben utilizar funciones que realicen el escapado de caracteres especiales, ya que no serán válidas en codificaciones multibyte (SJIS, BIG5, GBK, GB18030, UHC). | ☒ | No se utilizan funciones que realicen el escapado de caracteres especiales | Baja |
| **SEG-24** | El código fuente no debe contener cadenas de texto que se utilicen para formar sentencias SQL. | ☒ | | Baja |
| **SEG-25** | El uso de caracteres especiales (< , > , '' , ' , ( , ) , / , & , ;) no debe llevar a errores que provoquen la visualización del código fuente de la aplicación. | ☒ | | Baja |
| **SEG-26** | Se debe verificar la correcta validación de meta caracteres ( "",/,>,<,.. ) primero en el cliente y, a continuación, en el servidor. | ☒ | | Baja |
| **SEG-27** | Ejecución de ficheros malintencionados: La aplicación no debe permitir la ejecución de archivos locales en el servidor, ni la ejecución de archivos remotos. | ☒ | La aplicación solo admite ficheros en formato PDF | Alta |
| **SEG-28** | Falsificación de Petición en Sitios Cruzados (CSRF): La aplicación no debe atender peticiones http procedentes de páginas ajenas a la aplicación. | ☒ | | Baja |
| **SEG-29** | Referencia Directa a Objetos Insegura: Los parámetros de las URLS no deben hacer referencia directamente a ningún recurso, sino que debe hacerlo indirectamente mediante un identificador. | ☒ | | Alta |
| **SEG-30** | Referencia Directa a Objetos Insegura: Comprobar que no se pueden acceder a recursos ajenos al usuario indicando únicamente su identificador. | ☒ | | Alta |
| **SEG-31** | Buffer Overflow: En caso de que la aplicación utilice código nativo compilado, debe evitar que los usuarios puedan producir un buffer overflow. | ☒ | | Alta |

| Indicadores de revisión de seguridad | | | | |
|---|---|---|---|---|
| **Código** | **Descripción del Indicador** | **¿Cumple?** | **Observaciones** | **Severidad** |
| **SEG-32** | Open Redirect / CSR (Cross Site Redirect) | ☒ | Se han eliminado todos los enlaces directos hacia recursos URL, convirtiendo dichos accesos en reglas de navegación manejadas por la aplicación. | Alta |
| **SEG-33** | Vulnerabilidades a través de servicios web | ☒ | La Ventanilla Electrónica provee tres servicios web que están debidamente securizados mediante intercambio de certificados digitales X509. | Critica |
| **SEG-34** | Ficheros adjuntos | ☒ | No se requiere analizar el contenido de los ficheros adjuntos, la aplicación controla tamaño y extensión de fichero permitido. | Alta |
| **SEG-35** | Transmisiones no cifradas | ☒ | La aplicación no fuerza al usuario a conectarse mediante https. Sera responsabilidad del organismo realizar las configuraciones necesarias en el servidor de aplicaciones para atender todas las peticiones bajo protocolo seguro https | Media |
| **SEG-36** | Directory traversal | ☒ | Se han eliminado todos los enlaces directos hacia recursos URL, convirtiendo dichos accesos en reglas de navegación manejadas por la aplicación. | Baja |
| **SEG-37** | Cifrados de ficheros en base de datos | ☒ | La dirección de proyecto no considera adecuado cifrar los ficheros en la base de datos. | Baja |
| **SEG-38** | Fuga de información | ☒ | La aplicación no dispone de modo demostración por lo que solo trata datos reales. | Baja |

En la tabla siguiente se muestra el total de incumplimientos, organizados por severidad:

| Severidad | Nº incumplimientos | Indicadores |
|---|---|---|
| Alta | 0 | |
| Media | 0 | |
| Baja | 0 | |

Por tanto, se concluye que el nivel de seguridad es adecuado, el producto software es **ACEPTADO** atendiendo a sus aspectos de seguridad.

# 3 ANÁLISIS DE LOS INCUMPLIMIENTOS

N/A

# 4 CONCLUSIONES

Tras la finalización de las tareas necesarias para resolver los incumplimientos detectados, se han obtenido unos resultados satisfactorios, ya que no se detecta ninguna posible vulnerabilidad en la aplicación.

Por tanto, se concluye que la aplicación "Ventanilla Electrónica" es considerada como **apta**, atendiendo a los indicadores definidos para su aplicación en la presente auditoría de seguridad.

# 5 GLOSARIO

| **Término** | **Descripción** |
|---|---|
| VEA | Ventanilla Electrónica |
| OWASP | Open Web Application Security Project |

# 6 BIBLIOGRAFÍA Y REFERENCIAS

| Referencia | Título | Código |
|---|---|---|
| - | - | - |