AUDITORÍAS TÉCNICAS PARA LA CERTIFICACIÓN DE LOS SISTEMAS DE RECOGIDA DE INICIATIVAS CIUDADANAS EUROPEAS

Las auditorias técnicas según el Reglamento 211/2011 de la Unión Europea y según el Reglamento de Ejecución 1179/2011 de la Unión Europea donde se especifican los requisitos técnicos del artículo 6 del Reglamento 211/2011, deberán aportar el resultado de las siguientes comprobaciones:

A. Pruebas Funcionales.

En las aplicaciones web destinadas a la recogida de apoyos para las iniciativas ciudadanas europeas y afectadas por los Reglamentos 211/2011 y 1179/2011, se realizaran pruebas funcionales destinadas a asegurar que la funcionalidad de la aplicación web es la adecuada para la recogida de declaraciones de apoyo a través de la web.

Para llevar a cabo esta tarea se elaborara una lista de control o checklist que aborde los siguientes aspectos:

- Análisis de documentación y requisitos funcionales
- Diseño y realización de pruebas funcionales. En concreto se comprobara que:
    - La finalidad de la aplicación sea exclusivamente la recogida de apoyos y no contiene otras funcionalidades.
    - El interfaz de administración ("*backend*") este separado del área pública de recogida de apoyos.
    - La aplicación detecta e impide los apoyos duplicados.
    - La aplicación impide la presentación automatizada de declaraciones de apoyo.

- La aplicación genera informes de los firmantes de declaraciones de apoyo por cada Estado miembro.
- Permite la exportación en formato XML.
- La información exportada este marcada con la etiqueta de distribución limitada al estado miembro que la trate y como datos personales.

- Elaboración y Entrega del checklist de pruebas funcionales

B. Pruebas dinámicas de Seguridad.

Se realizaran pruebas dinámicas de seguridad sobre las aplicaciones web destinadas a identificar las posibles debilidades y vulnerabilidades de la misma. Las pruebas consistirán en las siguientes tareas:

- Análisis de vulnerabilidades: Se trata de una toma de datos sobre las vulnerabilidades (propias, tecnológicas y no tecnológicas) de los aplicativos implicados en el proyecto. Esta actividad se desarrollará con la asistencia de herramientas software diseñadas a tal efecto.
- Test de intrusión: Adicionalmente, se realizará una explotación profunda de las vulnerabilidades existentes mediante pruebas manuales de “Hacking” o intrusión en los aplicativos, obteniendo datos de mayor profundidad que los obtenidos en el análisis de vulnerabilidades.

  En estos test de intrusión se realizaran pruebas específicas para verificar el cumplimiento de las medidas de seguridad técnicas descritas en el reglamento 1179/2011. En concreto se realizaran pruebas para verificar la seguridad de:

  - Ataques de inyección tipo: *SQL, XPATH, LDAP*, comandos de sistema, etc.
  - Ataques de XSS (Cross-Site Scripting).
  - Control las sesiones (caducidad, aleatoriedad y tamaño de identificadores, etc.) y autenticación de la aplicación.
  - Ataques CSRF (Cross-site Request Forgery).
  - Elevación de privilegios en los permisos de usuario.

- Cifrado de las comunicaciones con la aplicación (correcta implementación HTTPS utilizando las configuraciones más seguras).
- Cifrado de las comunicaciones en los accesos remotos al sistema o en las comunicaciones con los estados miembros.
- Utilización de redirecciones o reenvíos no validados.
- Comprobación de fugas de información mediante la información proporcionada por los errores de la aplicación.
- Ataques definidos en el *"Top 10 de OWASP".*

Todas estas pruebas se realizaran de acuerdo con los estándares y metodologías definidos en las guías de pruebas de seguridad definidas por *OWASP.*

- Elaboración del informe de pruebas de seguridad: con el detalle de las vulnerabilidades y debilidades identificadas y un listado de recomendaciones y soluciones

C. Pruebas estáticas de Seguridad.

Se evaluara la seguridad de las aplicaciones de forma interna a través de pruebas y evaluaciones de seguridad a partir del código fuente de las mismas, identificando internamente las posibles debilidades y vulnerabilidades que puedan estar presentes en el código de las aplicaciones.

Para realizar esta tarea se realizara una revisión de la documentación con las especificaciones de las aplicaciones y se auditara el código de las mismas. La auditoria del código se realizara mediante la utilización de herramientas específicas para tal efecto y mediante la evaluación de los resultados por parte del equipo de trabajo.

Entre las pruebas que se realizaran, de acuerdo con el Reglamento 1179/2011 se incluyen las siguientes:

- Verificación de los algoritmos de cifrado utilizados internamente en la aplicación, tanto para el almacenamiento de la información en la base de datos, incluyendo las claves de usuarios, como para los procesos de autenticación y trasmisión de la información.
- Comprobación de mecanismos de depuración, gestión de errores y registro de actividades realizadas (trazas en los log) especialmente que se registren los accesos fallidos o exitosos a los datos.
- Verificación de los algoritmos utilizados para la generación de identificación, control de sesiones y gestión de claves.
- Comprobación de los mecanismos de etiquetado de información empleados.
- Verificación de la validación de entradas y salidas de la aplicación, así como las referencias a objetos.

Todas estas pruebas se de acuerdo con los estándares y metodologías definidos por las guías de desarrollo seguro elaboradas por *OWASP*.

Como resultado de estas pruebas se emitirá un informe que recoja el detalle de las vulnerabilidades encontradas con casos concretos donde se producen las vulnerabilidades, así como recomendaciones para su corrección. Este informe también servirá para intentar evidenciar mediante fallos en el código de la aplicación los resultados obtenidos en las pruebas dinámicas realizadas.

D. Evaluaciones de medidas organizativas y requisitos de seguridad.

La infraestructura IT en la que se instala y aloja la aplicación web también debe cumplir unas políticas y medidas de seguridad, tanto físicas como lógicas, adecuadas para garantizar el nivel de seguridad de la aplicación.

Estas políticas y medidas de seguridad serán evaluadas mediante una revisión documental de las mismas y una revisión de la aplicación en los entornos IT que alojan la aplicación web, según proceda.

Entre las medias que se comprobaran están las siguientes:

- Evaluación del cumplimiento de la norma ISO/IEC 27001, en especial la evaluación de riesgos, el plan de tratamiento de riesgos y el riesgo residual, teniendo en cuenta tanto la metodología de análisis de riesgos como que el análisis de amenazas sea exhaustivo y coherente.
- El plan de seguridad y las salvaguardas aplicadas en función de la categorización de la información y de los riesgos asociados, espacialmente la idoneidad y coherencia con el análisis de riesgos.
- La política de seguridad, y las normativas y procedimientos asociados, en particular la asignación de roles, la normativa de cifrado y etiquetado de información, de destrucción de información, de monitorización y gestión de trazas y eventos, la política de actualizaciones de parches y la política de copias de seguridad.
- Evaluación de controles de acceso físico a las instalaciones.
- Evaluación de parches y actualizaciones aplicados, tanto en sistema operativo, como base de datos y servidor de aplicaciones.
- Evaluación de controles de seguridad tanto lógicos en los sistemas, como de seguridad perimetral en la red, (cortafuegos empleados, ubicación en el segmento de red DMZ, etc.) o como la configuración de seguridad aplicada en particular las medidas de bastionado incluyendo la ejecución del servicio web por un usuario no privilegiado.
- Respecto a las copias de seguridad y cifrado de información se evaluara que tanto las copias de seguridad como los registros de auditoría estén adecuadamente protegidos mediante la utilización de mecanismos de cifrado.
- Evaluación de cumplimiento de requisitos legales, en particular el cumplimiento de la legislación de protección de datos de carácter personal y el documento de seguridad donde se recoja las medidas aplicadas en función de la categorización de la información.
- Evaluación de los diferentes Acuerdos de Nivel de Servicio (ANS) con los proveedores para garantizar la confidencialidad y trazabilidad de la

información, así como que la ubicación física de la información no se encuentre en un tercer país con una legislación no equiparable a la europea.

E. Requisitos del equipo que realice la auditoría

El equipo que realice la auditoría en los sistemas de Iniciativa Ciudadana Europea debe cumplir con los siguientes requisitos:

- **Los auditores:**
  - Todos los auditores tendrán certificación CISA y CISM o equivalentes.
  - El auditor jefe tendrá una experiencia mínima demostrable de 5 años como auditor jefe en auditorías dentro del ámbito de sistemas de gestión de la seguridad de la información. Dedicará un mínimo del 15% del tiempo de auditoría.
  - Los auditores tendrán 3 años mínimos de experiencia profesional demostrable en auditorías en el área de las tecnologías de la información y las comunicaciones
  - Al menos uno de los auditores tendrá 3 años mínimos de experiencia en el área jurídica (LOPD).

- **El personal técnico de seguridad:**
  - Que realice el test de penetración/hacking ético deberá tener:
    - experiencia demostrable como mínimo en los 3 últimos años
    - experiencia demostrable en ataques de explotación de las 10 mayores vulnerabilidades OWASP (OWASP top 10).
  - Que realice el análisis del código del aplicativo (si no se utiliza el software proporcionado por la comisión), deberá tener experiencia demostrable en desarrollo de aplicaciones bajo las recomendaciones OWASP.