******

***Informe de Auditoría de Seguridad***

*{nombre-url}*

***Grupo COFARES***

*Versión: 1.1*

*{date}*

| **Título** | **Informe de Auditoría de Seguridad** | | |
| --- | --- | --- | --- |
| **Elaborado** | Ciberseguridad | | |
| **Responsable** | URJC | | |
| **Fecha de elaboración** | {date} | | |
| **Metodología** | OWASP | | |
| Control de Versiones | | | |
| **Ver.** | **Fecha** | **Autor** | **Modificaciones** |
| 1.0 | {date} | Ciberseguridad | Creación de informe |

**Índice**

[1. Alcance 3](#_2f27goc7hkzp)

[2. Metodología 3](#_jogkx3bkifkm)

[3. Resumen Ejecutivo 4](#_yamd1ycorjl6)

[4. Resumen de vulnerabilidades 5](#_c4da2ptrp429)

[5. Análisis de Vulnerabilidades 6](#_qt3k68oxtwam)

[6. Checklist Requerimientos de Seguridad Web 14](#_odg7dn46onvu)

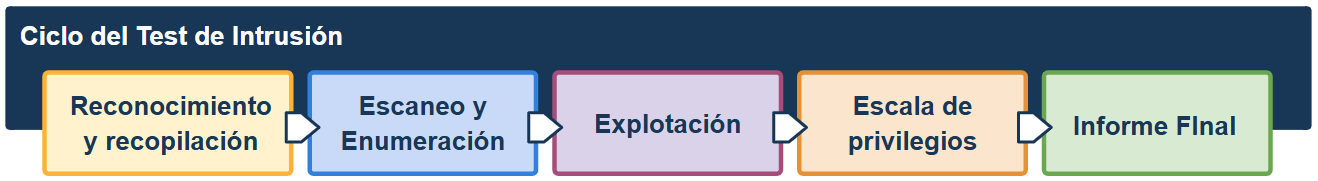
| **1. Alcance** |
| --- |

La presente auditoría tiene como alcance la evaluación de vulnerabilidades y requisitos de seguridad de la plataforma web {url}. Con el objetivo de no causar interrupciones de servicio en la plataforma de producción, la auditoría se ha llevado a cabo en el entorno de preproducción que corresponde con {url}

Se ha seguido una modalidad de auditoría de caja gris, en la que se ha facilitado información acerca de los activos a auditar incluyendo información técnica, servicios instalados, usuarios y contraseñas para acceder a la plataforma.

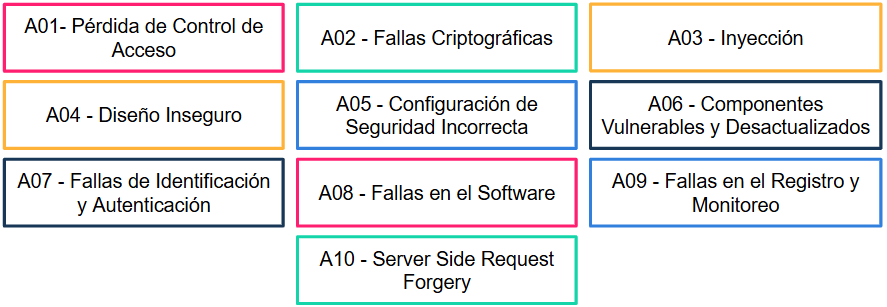
| **2. Metodología** |
| --- |

Las acciones y tareas realizadas en la auditoría se han llevado a cabo siguiendo una metodología propia de un ciclo de test de intrusión, junto con la metodología de auditoría web dictada por el estándar de seguridad OWASP, siguiendo las siguientes fases y actividades:



Adicionalmente, se han llevado a cabo pruebas manuales para identificar problemas de flujo de datos, lógica empresarial y control de acceso, todo ello recogido en el checklist de requerimientos de seguridad web.

En cuanto a la metodología OWASP, se ha clasificado las vulnerabilidades siguiendo la guía OWASP Top 10, en las que se enumeran los riesgos más críticos para la seguridad de las aplicaciones web:



Adicionalmente, para cada vulnerabilidad identificada se ha detallado proporcionando las evidencias correspondientes, el riesgo que supone, propuestas de solución y/o mitigación y enlaces de interés; junto con la calificación de la criticidad del impacto de la vulnerabilidad siguiendo la siguiente tabla:

| **Impacto** | **Definición** |
| --- | --- |
| **Alta** | Vulnerabilidad crítica que permite comprometer completamente el sistema, acceder a datos sensibles, realizar cambios no autorizados o interrumpir servicios esenciales. |
| **Media** | Vulnerabilidad significativa que puede ser explotada para obtener ventajas parciales o causar daños moderados. |
| **Baja** | Vulnerabilidad de bajo riesgo que puede ser explotada, pero requiere condiciones muy específicas o tiene un impacto limitado. |
| **Informativa** | Hallazgos que no representan una amenaza directa, pero pueden proporcionar información útil para un atacante o ser considerados buenas prácticas de remediación. |

| **3. Resumen Ejecutivo** |
| --- |

{resumen\_ejecutivo}

| **4. Resumen de vulnerabilidades** |
| --- |
|  |

| **Vulnerabilidad** | **Nº Alertas** | **Categoría**  **OWASP** | **Criticidad** | **Estado** |
| --- | --- | --- | --- | --- |

| **5. Análisis de Vulnerabilidades** |
| --- |
| A continuación, se detallan las vulnerabilidades identificadas durante la auditoría de seguridad. Para cada vulnerabilidad, se incluye una descripción del problema, el riesgo asociado, así como recomendaciones y medidas correctoras. Además, se proporcionan enlaces de interés con recursos adicionales que permiten profundizar en la comprensión de cada vulnerabilidad y en las mejores prácticas para su remediación. |

| **[VULN-{numero}] {alert\_name}** | | | |
| --- | --- | --- | --- |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **{risk}** | {owasp} | {cwe} | {url} |
| **Detalles** |  | | |
| {detalles} | | | |
| **Riesgo** |  | | |
| {riesgo} | | | |
| **Solución** |  | | |
| {solucion} | | | |
| **Referencias** |  | | |
| {referencias} | | | |