

***Informe de Auditoría de Seguridad***

*{nombre-url}*

***Grupo COFARES***

*Versión: 1.1*

*{date}*

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

**Índice**

[1. Alcance 3](#_p4oemcyod1zt)

[2. Metodología 3](#_dacxzmujloap)

[3. Resumen Ejecutivo 4](#_1as8lml38neq)

[4. Resumen de vulnerabilidades 5](#_hhrdc86cfmqi)

[5. Análisis de Vulnerabilidades 6](#_8w3sct9ttwb9)

[6. Checklist Requerimientos de Seguridad Web 14](#_zfy2iuy1adz0)

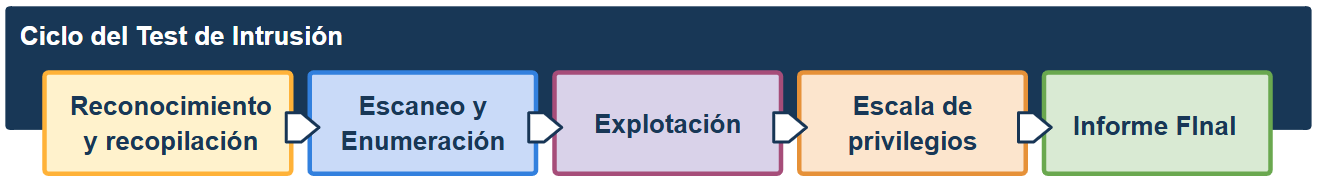
|  |
| --- |
| **1. Alcance** |

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.

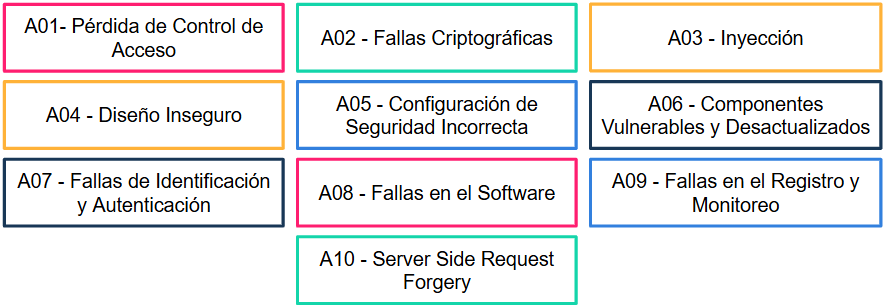
|  |
| --- |
| **2. Metodología** |

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:

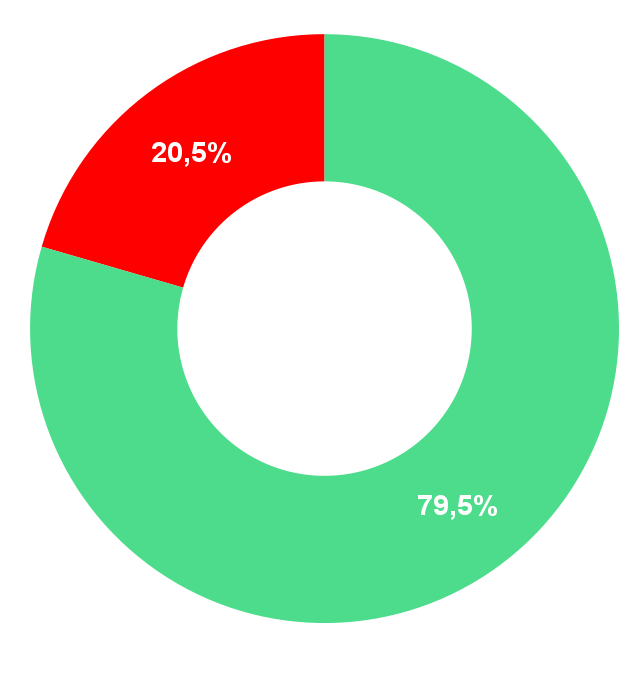
|  |  |
| --- | --- |
| **Impacto** | **Definición** |
| **Alta** | Vulnerabilidad crítica que permite comprometer completamente el sistema, acceder a datos sensibles, realizar cambios no autorizados o interrumpir servicios esenciales. |
| **Media** | Vulnerabilidad significativa que puede ser explotada 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** |
|  |

**Evaluación de Requerimientos de Seguridad Web**

**Cumple / No cumple**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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} | | | |

|  |
| --- |
| **6. Checklist Requerimientos de Seguridad Web** |

En este apartado se detalla un checklist de requerimientos que contempla los principales controles y buenas prácticas que deben ser evaluados para garantizar un entorno seguro y robusto frente a posibles amenazas.

Se estructura en categorías clave que cubren aspectos críticos de la aplicación, tales como el control de acceso y autenticación, la gestión de sesiones y cookies, la configuración adecuada de cabeceras HTTP, el manejo seguro de transacciones y entradas de datos, así como mecanismos de protección activa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Tipo**  **Requerimiento** | **Requisito de Seguridad** | **Cumple** | **Criticidad** |
| 1 | **Control de acceso y autenticación** | Autenticación total para todos los recursos/páginas | **SI** | **Baja** |
| Es necesario estar autenticado para acceder a cada uno de los recursos y/o página de la plataforma. | | |
| 2 | Doble verificación para el registro o alta | **SI** | **Media** |
| Se solicita un código OTP en el primer inicio de sesión tras el registro de un nuevo usuario. | | |
| 3 | Política de complejidad de contraseña | **SI** | **Alta** |
| La política de contraseña establecida es: 5-8 caracteres de longitud, donde se debe incluir como mínimo una letra mayúscula, una letra minúscula y un número. | | |
| 4 | Renovación periódica de contraseña | **NO** | **Media** |
| No hay un mecanismo para la renovación periódica de contraseñas. | | |
| 5 | Autenticación Multifactor opcional para cuentas de usuarios | **NO** | **Media** |
| No existe autenticación multifactor para el inicio de sesión de los usuarios en la plataforma. | | |
| 6 | Autenticación Multifactor para cuentas administrador | **NO** | **Crítica** |
| No existe autenticación multifactor para el inicio de sesión de los administradores en la plataforma. | | |
| 7 | Autenticación Multifactor en zonas con información sensible o datos bancarios | **SI** | **Crítica** |
| transferencias, reseteo. consulta. | | |
| 8 | Mecanismo Captcha para la autenticación | **SI** | **Baja** |
| En caso de introducir incorrectamente la contraseña, en el siguiente inicio de sesión se solicita completar un mecanismo captcha. | | |
| 9 | Mecanismo Captcha para el registro/alta | **SI** | **Baja** |
| El registro debe validarse mediante el envío de un código OTP. | | |
| 10 | Bloqueo de cuenta tras intentos fallidos | **SI** | **Media** |
| Se ha comprobado que tras varios intentos fallidos de autenticación, la cuenta de usuario es bloqueada. | | |
| 11 | Función de recordatorio/olvido de contraseña válido | **SI** | **Media** |
| El mecanismo de reseteo de contraseña es lo suficientemente seguro, incluyendo un mecanismo multifactor de autenticación OTP para validar la acción. | | |
| 12 | Doble verificación para el cambio/reseteo de contraseña | **SI** | **Alta** |
| Se solicita un código OTP para validar el cambio/reseteo de contraseña. | | |
| 13 | Contraseña temporal o link temporal para el cambio de contraseña | **N/A** | **Alta** |
| No aplica. El cambio de contraseña se lleva a cabo en el mismo portal de Sección de Crédito tras ser validado por el código OTP. | | |
| 14 | Histórico de 3 o más contraseñas para el cambio/reseteo de contraseña | **NO** | **Media** |
| Únicamente te prohíbe establecer la misma contraseña igual a la última. | | |
| 15 | Respuestas de error genéricas en la autenticación | **SI** | **Baja** |
| La respuesta de error tras un intento de inicio de sesión fallido es genérica. *“La autenticación ha fallado. Por favor inténtelo otra vez”* | | |
| 16 | Respuestas de error genéricas en el servicio de cambio de contraseña | **SI** | **Baja** |
|  | | |
| 17 | Almacenamiento y cifrado seguro de contraseñas | **SI** | **Media** |
|  | | |
| 18 | Registro de eventos de seguridad | **SI** | **Media** |
|  | | |
| 19 | **Gestión de sesión y cookies** | El cierre de sesión termina con la sesión/conexión asociada | **SI** | **Alta** |
| Se ha comprobado que el cierre de sesión se completa correctamente y la sesión se destruye. | | |
| 20 | Tiempo de vida de sesión | **SI** | **Media** |
|  | | |
| 21 | Cierre de sesión automático tras expiración de sesión | **SI** | **Media** |
|  | | |
| 22 | Generación de nuevos identificadores por sesión | **SI** | **Baja** |
|  | | |
| 23 | Tokens CSRF | **NO** | **Baja** |
| Se detalla en la vulnerabilidad [VULN-03]. | | |
| 24 | No existe información sensible o confidencial en cookies | **SI** | **Baja** |
|  | | |
| 25 | Cookies con atributo Secure configurado | **NO** | **Baja** |
| Se detalla en la vulnerabilidad [VULN-04]. | | |
| 26 | Cookies con atributo HttpOnly configurado | **SI** | **Baja** |
|  | | |
| 27 | Cookies con attribute SameSite Flag | **NO** | **Baja** |
| Se detalla en la vulnerabilidad [VULN-05]. | | |
| 28 | **Gestión y configuración de cabeceras HTTP** | HTTP Strict Transport Security (HSTS) | **SI** | **Baja** |
|  | | |
| 29 | X-XSS-Protection | **NO** | **Media** |
| Se detalla en la vulnerabilidad [VULN-01] | | |
| 30 | X-Content-Type-Options | **SI** | **Baja** |
|  | | |
| 31 | X-Frame-Options | **SI** | **Media** |
|  | | |
| 32 | Content Security Policy (CSP) | **SI** | **Baja** |
|  | | |
| 33 | Cache Control | **SI** | **Baja** |
|  | | |
| 34 | Cross-Origin-Resource-Policy (CORP) | **SI** | **Baja** |
|  | | |
| 35 | **Transacción y entrada de datos** | Protocolo HTTPS TLS seguro (TLSv1.3 o TLSv1.2) | **SI** | **Alta** |
| https://www.ssllabs.com/analyze.html?d=sdc30.cofares.es&latest | | |
| 36 | Certificado SSL válido y bien configurado | **SI** | **Media** |
| La calificación otorgada por el escaner ssllabs es de A+. | | |
| 37 | Validación de entrada de datos | **SI** | **Media** |
| Parcialmente. Revisar vulnerabilidad [VULN-01] | | |
| 38 | Validación de subida/carga de ficheros | **N/C** | **Media** |
| No existe la carga o subida de ficheros a la plataforma. | | |
| 39 | Mensaje de error tras la entrada de datos ilegítimas o malformadas | **SI** | **Baja** |
|  | | |
| 40 | Límite de transacciones/peticiones en un periodo de tiempo | **SI** | **Media** |
| Es posible configurar un límite de transacciones web por usuario. | | |
| 42 | **Protección Activa** | Protección WAF | **SI** | **Media** |
|  | | |