

***Informe de Auditoría de Seguridad***

https://example.com

***Grupo COFARES***

*Versión: 1.1*

23/04/2025

|  |  |  |  |
| --- | --- | --- | --- |
| **Título** | **Informe de Auditoría de Seguridad** | | |
| **Elaborado** | Ciberseguridad | | |
| **Responsable** | Pedro Iván Montes | | |
| **Fecha de elaboración** | 23/04/2025 | | |
| **Metodología** | OWASP | | |
| Control de Versiones | | | |
| **Ver.** | **Fecha** | **Autor** | **Modificaciones** |
| 1.0 | 23/04/2025 | 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)

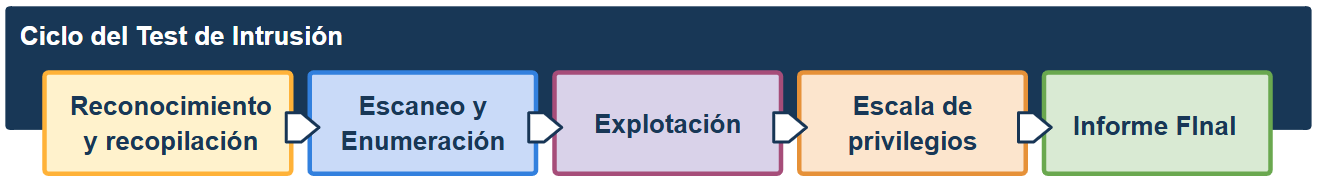
|  |
| --- |
| **1. Alcance** |

La presente auditoría tiene como alcance la evaluación de vulnerabilidades y requisitos de seguridad de la plataforma web https://example.com. 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 https://example.com

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.

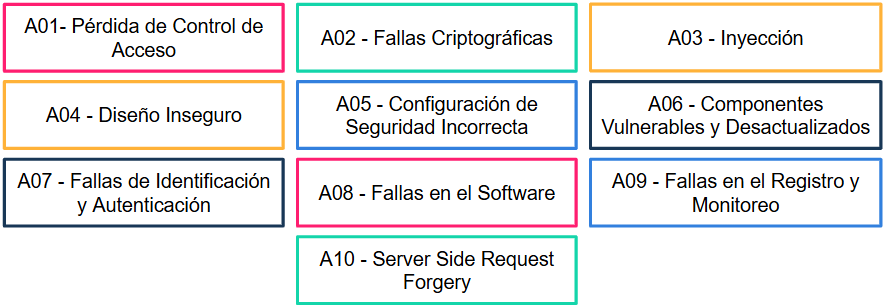
|  |
| --- |
| **2. Metodología** |

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:

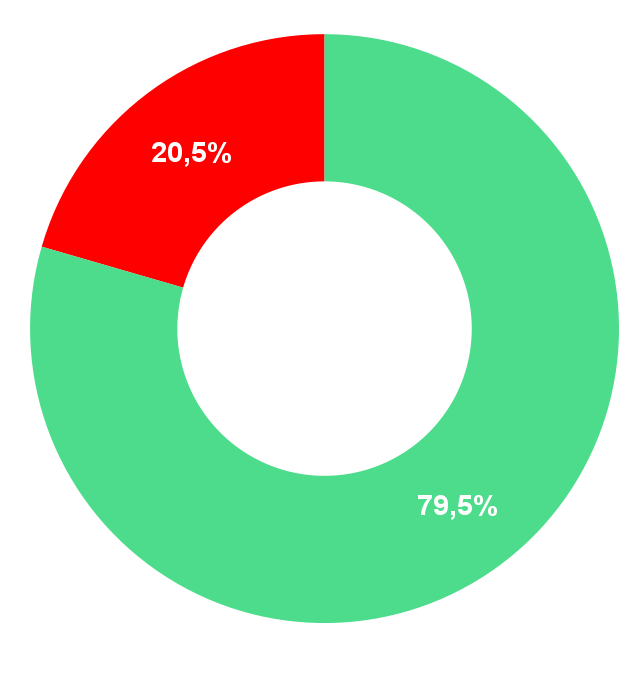
|  |  |
| --- | --- |
| **Impacto** | **Definición** |
| **Alta** | Vulnerabilidad crítica que permite comprometer completamente el sistema, acceder a datos sensibles, realizar cambios no autorizados o interrumpir servicios esenciales. |
| **Media** | Vulnerabilidad significativa que puede ser explotada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

La auditoría de seguridad en example.com reveló áreas de mejora en la protección de la información y la experiencia del usuario. Si bien el sitio web funciona correctamente, se identificaron configuraciones que podrían ser aprovechadas por atacantes para realizar acciones maliciosas.  
  
En particular, faltan cabeceras de seguridad esenciales que ayudan a los navegadores a proteger a los usuarios de ataques comunes. La ausencia de la cabecera "X-Content-Type-Options" permite la inyección de contenido no deseado. La falta de "Content Security Policy (CSP)" dificulta la prevención de ataques de scripting entre sitios (XSS). La no implementación de "Strict-Transport-Security (HSTS)" expone a los usuarios a ataques "Man-in-the-Middle". Finalmente, la falta de una cabecera anti-clickjacking facilita el engaño a los usuarios para realizar acciones no deseadas.  
  
Recomendamos implementar estas cabeceras lo antes posible. Estas medidas, aunque sencillas, refuerzan significativamente la seguridad del sitio web y la confianza de los usuarios. La revisión de las directivas de caché también podría optimizar el almacenamiento de información sensible en el navegador.

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

**Evaluación de Requerimientos de Seguridad Web**

**Cumple / No cumple**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerabilidad** | **Nº Alertas** | **Categoría**  **OWASP** | **Criticidad** | **Estado** |
| [VUL 01] Missing Anti-clickjacking Header | 1 | A05 | Medio | Detectada |
| [VUL 02] Content Security Policy (CSP) Header Not Set | 1 | A05 | Medio | Detectada |
| [VUL 03] Strict-Transport-Security Header Not Set | 1 | A06 | Bajo | Detectada |
| [VUL 04] X-Content-Type-Options Header Missing | 1 | A07 | Bajo | Detectada |
| [VUL 05] Re-examine Cache-control Directives | 1 | A05 | Informativo | Detectada |
| [VUL 01] Missing Anti-clickjacking Header | 1 | A05 | Medio | Detectada |
| [VUL 02] Content Security Policy (CSP) Header Not Set | 1 | A05 | Medio | Detectada |
| [VUL 03] Strict-Transport-Security Header Not Set | 1 | A03 | Bajo | Detectada |
| [VUL 04] X-Content-Type-Options Header Missing | 1 | A05 | Bajo | Detectada |
| [VUL 05] Re-examine Cache-control Directives | 1 | A05 | Informativo | Detectada |

|  |
| --- |
| **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-01] Missing Anti-clickjacking Header** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 1021 | https://example.com |
| **Detalles** |  | | |
| La ausencia de la cabecera Anti-clickjacking permite que un atacante pueda superponer capas maliciosas sobre la interfaz web legítima, engañando a los usuarios para que realicen acciones sin su consentimiento. Esta técnica, conocida como clickjacking, puede llevar al robo de credenciales, la manipulación de datos o la ejecución de acciones no deseadas en nombre del usuario. | | | |
| **Riesgo** |  | | |
| El principal riesgo es la manipulación de la interfaz de usuario, lo que permite a un atacante engañar al usuario para realizar acciones involuntarias. Esto puede resultar en el robo de información confidencial, la modificación no autorizada de la configuración de la cuenta o la ejecución de transacciones fraudulentas, dañando la reputación y la confianza del usuario en la aplicación. | | | |
| **Solución** |  | | |
| Implementar la cabecera 'X-Frame-Options' con las directivas 'DENY' o 'SAMEORIGIN' para evitar que la página se cargue dentro de un iframe en dominios no autorizados. Considerar 'Content-Security-Policy' con la directiva 'frame-ancestors' como una alternativa más flexible y robusta para controlar el embedding de la página en otros sitios web. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-01] Missing Anti-clickjacking Header** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 1021 | https://example.com |
| **Detalles** |  | | |
| La ausencia de la cabecera Anti-clickjacking permite que un atacante pueda superponer capas maliciosas sobre la interfaz web legítima, engañando a los usuarios para que realicen acciones sin su consentimiento. Esta técnica, conocida como clickjacking, puede llevar al robo de credenciales, la manipulación de datos o la ejecución de acciones no deseadas en nombre del usuario. | | | |
| **Riesgo** |  | | |
| El principal riesgo es la manipulación de la interfaz de usuario, lo que permite a un atacante engañar al usuario para realizar acciones involuntarias. Esto puede resultar en el robo de información confidencial, la modificación no autorizada de la configuración de la cuenta o la ejecución de transacciones fraudulentas, dañando la reputación y la confianza del usuario en la aplicación. | | | |
| **Solución** |  | | |
| Implementar la cabecera 'X-Frame-Options' con las directivas 'DENY' o 'SAMEORIGIN' para evitar que la página se cargue dentro de un iframe en dominios no autorizados. Considerar 'Content-Security-Policy' con la directiva 'frame-ancestors' como una alternativa más flexible y robusta para controlar el embedding de la página en otros sitios web. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-01] Missing Anti-clickjacking Header** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 1021 | https://example.com |
| **Detalles** |  | | |
| La ausencia de la cabecera Anti-clickjacking permite que un atacante pueda superponer capas maliciosas sobre la interfaz web legítima, engañando a los usuarios para que realicen acciones sin su consentimiento. Esta técnica, conocida como clickjacking, puede llevar al robo de credenciales, la manipulación de datos o la ejecución de acciones no deseadas en nombre del usuario. | | | |
| **Riesgo** |  | | |
| El principal riesgo es la manipulación de la interfaz de usuario, lo que permite a un atacante engañar al usuario para realizar acciones involuntarias. Esto puede resultar en el robo de información confidencial, la modificación no autorizada de la configuración de la cuenta o la ejecución de transacciones fraudulentas, dañando la reputación y la confianza del usuario en la aplicación. | | | |
| **Solución** |  | | |
| Implementar la cabecera 'X-Frame-Options' con las directivas 'DENY' o 'SAMEORIGIN' para evitar que la página se cargue dentro de un iframe en dominios no autorizados. Considerar 'Content-Security-Policy' con la directiva 'frame-ancestors' como una alternativa más flexible y robusta para controlar el embedding de la página en otros sitios web. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-01] Missing Anti-clickjacking Header** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 1021 | https://example.com |
| **Detalles** |  | | |
| La ausencia de la cabecera Anti-clickjacking permite que un atacante pueda superponer capas maliciosas sobre la interfaz web legítima, engañando a los usuarios para que realicen acciones sin su consentimiento. Esta técnica, conocida como clickjacking, puede llevar al robo de credenciales, la manipulación de datos o la ejecución de acciones no deseadas en nombre del usuario. | | | |
| **Riesgo** |  | | |
| El principal riesgo es la manipulación de la interfaz de usuario, lo que permite a un atacante engañar al usuario para realizar acciones involuntarias. Esto puede resultar en el robo de información confidencial, la modificación no autorizada de la configuración de la cuenta o la ejecución de transacciones fraudulentas, dañando la reputación y la confianza del usuario en la aplicación. | | | |
| **Solución** |  | | |
| Implementar la cabecera 'X-Frame-Options' con las directivas 'DENY' o 'SAMEORIGIN' para evitar que la página se cargue dentro de un iframe en dominios no autorizados. Considerar 'Content-Security-Policy' con la directiva 'frame-ancestors' como una alternativa más flexible y robusta para controlar el embedding de la página en otros sitios web. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-01] Missing Anti-clickjacking Header** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 1021 | https://example.com |
| **Detalles** |  | | |
| La ausencia de la cabecera Anti-clickjacking permite que un atacante pueda superponer capas maliciosas sobre la interfaz web legítima, engañando a los usuarios para que realicen acciones sin su consentimiento. Esta técnica, conocida como clickjacking, puede llevar al robo de credenciales, la manipulación de datos o la ejecución de acciones no deseadas en nombre del usuario. | | | |
| **Riesgo** |  | | |
| El principal riesgo es la manipulación de la interfaz de usuario, lo que permite a un atacante engañar al usuario para realizar acciones involuntarias. Esto puede resultar en el robo de información confidencial, la modificación no autorizada de la configuración de la cuenta o la ejecución de transacciones fraudulentas, dañando la reputación y la confianza del usuario en la aplicación. | | | |
| **Solución** |  | | |
| Implementar la cabecera 'X-Frame-Options' con las directivas 'DENY' o 'SAMEORIGIN' para evitar que la página se cargue dentro de un iframe en dominios no autorizados. Considerar 'Content-Security-Policy' con la directiva 'frame-ancestors' como una alternativa más flexible y robusta para controlar el embedding de la página en otros sitios web. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-02] Content Security Policy (CSP) Header Not Set** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 693 | https://example.com |
| **Detalles** |  | | |
| La ausencia de una cabecera Content Security Policy (CSP) en las respuestas del servidor web expone la aplicación a ataques de Cross-Site Scripting (XSS). Sin una CSP definida, el navegador permite la ejecución de scripts provenientes de cualquier origen, facilitando la inyección de código malicioso por parte de atacantes. Esto compromete la integridad y confidencialidad de los datos del usuario. | | | |
| **Riesgo** |  | | |
| La falta de una CSP efectiva permite la ejecución de scripts no autorizados, lo que puede resultar en el robo de credenciales, la manipulación del contenido de la página, el redireccionamiento a sitios maliciosos y la propagación de malware. Los usuarios pueden ser engañados para revelar información sensible, y la reputación de la aplicación puede verse gravemente dañada. | | | |
| **Solución** |  | | |
| Implementar una cabecera Content Security Policy (CSP) que especifique las fuentes válidas de contenido (scripts, estilos, imágenes, etc.). Definir una política restrictiva que permita únicamente el contenido necesario para la funcionalidad de la aplicación. Validar y ajustar la CSP de forma continua para asegurar su efectividad y evitar bloqueos innecesarios. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\_Content\_Security\_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content\_Security\_Policy\_Cheat\_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/ | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-03] Strict-Transport-Security Header Not Set** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Bajo** | A06 | 319 | https://example.com |
| **Detalles** |  | | |
| La falta de la cabecera HTTP Strict-Transport-Security (HSTS) permite ataques Man-in-the-Middle. Un atacante puede interceptar la conexión inicial HTTP y redirigir al usuario a una página HTTPS falsa. HSTS fuerza a los navegadores a usar siempre HTTPS, previniendo conexiones no seguras y protegiendo contra la suplantación. | | | |
| **Riesgo** |  | | |
| El principal riesgo es la exposición de datos sensibles transmitidos a través de HTTP en lugar de HTTPS. Un atacante podría interceptar información confidencial como contraseñas, cookies de sesión o datos personales. La ausencia de HSTS facilita ataques de downgrade, comprometiendo la confidencialidad e integridad de la comunicación. | | | |
| **Solución** |  | | |
| Implementar la cabecera HSTS en la configuración del servidor web. Establecer un tiempo máximo (max-age) adecuado, incluir subdominios (includeSubDomains) y considerar la directiva preload. Validar la configuración con herramientas de seguridad y monitorear regularmente para asegurar su persistencia y efectividad. | | | |
| **Referencias** |  | | |
| https://cheatsheetseries.owasp.org/cheatsheets/HTTP\_Strict\_Transport\_Security\_Cheat\_Sheet.html https://owasp.org/www-community/Security\_Headers https://en.wikipedia.org/wiki/HTTP\_Strict\_Transport\_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-04] X-Content-Type-Options Header Missing** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Bajo** | A07 | 693 | https://example.com |
| **Detalles** |  | | |
| La falta de la cabecera X-Content-Type-Options permite que el navegador interprete incorrectamente el tipo de contenido de los archivos, lo que puede llevar a ataques de cross-site scripting (XSS). Esta cabecera instruye al navegador para que respete el tipo de contenido especificado en la cabecera Content-Type, previniendo la ejecución de código malicioso. | | | |
| **Riesgo** |  | | |
| Si un atacante logra subir un archivo malicioso con una extensión legítima (ej. .jpg) pero con contenido HTML/JavaScript, el navegador podría interpretarlo como HTML debido a la falta de la cabecera, permitiendo la ejecución de código XSS. Esto puede llevar al robo de cookies, redirección a sitios maliciosos o la manipulación de la página web. | | | |
| **Solución** |  | | |
| Configurar el servidor web para que incluya la cabecera X-Content-Type-Options con el valor 'nosniff' en todas las respuestas HTTP. Esto forzará al navegador a respetar el tipo de contenido especificado en la cabecera Content-Type, evitando la interpretación incorrecta de los archivos y mitigando el riesgo de ataques XSS. | | | |
| **Referencias** |  | | |
| https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security\_Headers | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-05] Re-examine Cache-control Directives** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Informativo** | A05 | 525 | https://example.com |
| **Detalles** |  | | |
| Esta alerta indica una configuración inadecuada de las directivas 'Cache-Control'. La falta de configuración o una configuración permisiva permite que información sensible sea almacenada en caché por navegadores o proxies. Esto incrementa el riesgo de exposición de datos confidenciales a usuarios no autorizados, especialmente en redes compartidas o dispositivos comprometidos. Es crucial revisar y ajustar las directivas para un manejo seguro de la información en caché. | | | |
| **Riesgo** |  | | |
| El riesgo principal radica en la exposición de datos sensibles. Información como contraseñas, datos personales o financieros podría ser almacenada en caché de forma no segura. Esto facilita el acceso no autorizado a esta información por parte de atacantes o usuarios malintencionados que puedan acceder al caché. Esto puede resultar en robo de identidad, fraude financiero y otros delitos cibernéticos. | | | |
| **Solución** |  | | |
| Implementar directivas 'Cache-Control' robustas que definan explícitamente cómo se debe almacenar en caché la información. Utilizar 'no-cache', 'no-store', 'private' o 'max-age' para controlar el almacenamiento en caché de datos sensibles. Validar las directivas en el servidor y en el cliente para garantizar su correcta implementación. Implementar la directiva 'immutable' para recursos estáticos. | | | |
| **Referencias** |  | | |
| https://cheatsheetseries.owasp.org/cheatsheets/Session\_Management\_Cheat\_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/ | | | |

|  |
| --- |
| **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** |
|  | | |