# Conclusiones

La seguridad de la información ha sido un importante tema de debate desde el nacimiento de la tecnología, y seguirá siendo un tema importante en un futuro previsible. Los riesgos asociados con sistemas impropiamente mantenidos incluyen daños económicos y robos de información, y la llegada de Internet no ha hecho sino aumentar este riesgo y sus efectos potenciales a niveles nunca antes vistos. Ahora más que nunca, no debe desestimarse la importancia de la seguridad de la información.

En el caso particular de las empresas, un sistema vulnerable podría resultar en graves daños financieros y la pérdida de reputación asociada con el filtrado de información privada, que en algunos casos podría incluso tener repercusiones legales. Para pequeñas y medianas empresas en auge, este tipo de error podría resultar fatal, y podría herir gravemente sus posibilidades de crecer y volverse competitivas en una economía cambiante.

Si bien este proyecto se ha centrado en vulnerabilidades relacionadas con aplicaciones web en particular, esto no quiere decir que otros aspectos de la seguridad de la información no sean igual de importantes o deban ser desestimados. Sin embargo, el hecho de que las aplicaciones web estén constantemente expuestas a Internet las convierte en un objetivo atractivo para atacantes.

Como se mencionó en secciones anteriores, las estadísticas muestran que las empresas gastan menos en pruebas de aplicaciones web en comparación con otras formas de seguridad informática. Esto podría indicar una insuficiente concienciación acerca de la importancia de las aplicaciones web seguras, y de la seguridad de la información en general.

## Recomendaciones

El escáner de aplicaciones web desarrollado para este proyecto no debería verse como un sustituto de una prueba de penetración realizada por un profesional. Este escáner no puede detectar muchos tipos de vulnerabilidades, algunas debido a que el programa es bastante simple, y otras debido a que ciertos tipos de vulnerabilidades sencillamente no pueden ser detectadas mediante métodos automáticos. Puede verse como una forma económica de tantear el terreno, pero la única formar de certificar que una aplicación web es segura es contactando a un pen-tester profesional.

También cabría destacar que la invulnerabilidad completa es inalcanzable, pues siempre existirán nuevos vectores de ataque y circunstancias imprevistas. Aun así, pueden adoptarse buenas prácticas para minimizar riesgos, tales como:

* Es altamente recomendado tener un plan de seguridad detallando como emplear el presupuesto de seguridad y que individuos deberían ser responsables de que. Deberían fijarse prioridades respecto a las vulnerabilidades en función de su daño potencial y la facilidad de su explotación. Si una empresa cuenta con múltiples aplicaciones web, deberían ordenarse según su prioridad de una manera similar.
* Las cookies deberían usarse de manera segura. Nunca deberían guardar información confidencial, y deberían encriptarse siempre que fuera posible.
* Encriptar la URL puede ayudar a prevenir una variedad de diferentes ataques, como CSRF o escalado de directorios.
* La validación de datos puede ayudar a prevenir algunas de las formas de ataque más extendidas como XSS o inyección.
* Se recomienda el uso de HTTPS en lugar de HTTP.

Aunque estos pasos pueden ser costosos y pueden resultar en una infraestructura web más complicada, la aplicación web resultante será menos propensa a ser afectada por un ataque. Todo considerado, si bien no existe una solución sencilla al problema de la seguridad de las aplicaciones web, las auditorías periódicas pueden demostrar ser un método rentable para mantener los posibles riesgos bajo control.