Capítulo 5.

Conclusiones.

Durante este trabajo de tesis hemos tenido la posibilidad de valorar los diferentes estudios y criterios sobre la seguridad informática para aplicaciones basadas en Internet, para asegurar su confiabilidad y calidad. Desgraciadamente, los desperfectos de la seguridad se dan con mucha frecuencia, y los cortafuegos corporativos a menudo son inútiles cuando un hoyo de la seguridad existe en una aplicación. Sin embargo, existe la esperanza en la forma que **AppScan DE** ayuda a que los desarrolladores prueben sus aplicaciones en tiempo de diseño. **AppScan DE** es el primer instrumento de su clase que ayuda con esto. Permite a los desarrolladores a probar la seguridad cuando ellos están en el desarrollo de la aplicación, así como con en el producto terminado. Enseña e impone mejores prácticas que las organizaciones pueden construir en sus pautas del desarrollo y diseño.

Se llevó a cabo un análisis detallado de herramientas de apoyo para asegurar las Aplicaciones Web del CENTIA, particularmente **Manager PKI** y **AppScan DE**. La comparación de ambas se encuentra en el apéndice. Concluimos que **AppScan DE** podrá servir como base a futuras Aplicaciones Web. Por esto realizamos las siguientes recomendaciones:

1. El primer paso que se debe de seguir para asegurar una aplicación Web, es saber cuán vulnerable es. Cuando las aplicaciones llegan a ser más sofisticadas, las presiones del tiempo en el mercado son una parte cada vez más significativa de los problemas actuales de la seguridad. Además, cuanto más las compañías exponen sus sistemas a clientes, se hacen a sí mismas más responsables de la seguridad.

2. **AppScan DE** explora un sitio Web, busca potenciales defectos de seguridad, “ataca” el sitio basado en el conocimiento que reunió durante la búsqueda, e informa sus éxitos y los fracasos. De acuerdo con la investigación hecha en este trabajo de tesis, encontrar un defecto durante el despliegue de la aplicación es 100 veces más costoso que la modificación en el código en tiempo de diseño. Si no se resuelven estos problemas permitirán a piratas informáticos tomar

fácilmente un sistema, robar identidades e incluso cambiar los datos críticos **[Sanctum, 2004]**.

3. Con **AppScan DE**, los desarrolladores tienen acceso a un instrumento integrado que hace un código seguro que es una meta accesible, los clientes pueden recibir aplicaciones de calidad. Arreglar hoyos de seguridad en el despliegue de la aplicación es muy costoso, equiparse con una herramienta como esta será una fuerte inversión que ayudara a crear mejores y más seguras aplicaciones Web. **AppScan DE** puede hacer pruebas de defectos de seguridad mientras los desarrolladores trabajan en la aplicación. Esto se hace en tres pasos muy fáciles, como se muestra en la figura 5.1:

Figura 5.1. Pasos para detectar defectos de seguridad **[Sanctum, 2004]**.

4. **AppScan DE** es un instrumento para probar la seguridad de las aplicaciones Web. Al saber más del producto de **AppScan DE**, será difícil de evitar la impresión de que **AppScan DE** es como un tipo de "pirata informático". Es verdad en por lo menos un sentido**: AppScan DE** aplica el mismo tipo de técnicas como un pirata informático suele infiltrarse a un sitio Web. Afortunadamente, **AppScan DE** es un mecanismo benigno, no una persona malévola, porque hace su trabajo muy bien.

5. Otro resultado valioso en este trabajo ha sido el establecimiento de un conjunto de de lineamientos de seguridad para lograr la confiabilidad y calidad del software basado en Internet. No hay menor duda que si se siguen los lineamientos planteados en el capítulo 4, será cada vez menos la preocupación constante que tienen los investigadores del CENTIA de acuerdo a la seguridad de sus Aplicaciones Web, ya que estos lineamientos son un buen consejo para tener una seguridad aceptable en un sistema.

De esta manera, se concluye que **AppScan DE** es la mejor opción para asegurar las Aplicaciones Web del CENTIA descubriendo sus vulnerabilidades y generando recomendaciones para arreglarlas en la etapa de desarrollo y de algunas aplicaciones que ya han sido desplegadas y al mismo tiempo siguiendo los lineamientos que se plantearon en el capítulo 4, esto ahorrará tiempo y costos significativos para el CENTIA.