Conclusiones

La realización de este trabajo nos ha exigido una comprensión sensiblemente más profunda del funcionamiento de las redes de datos y los dispositivos que la conforman, los protocolos que se emplean en ellas, la seguridad en las mismas y algunas de las técnicas más utilizadas para violar dicha seguridad.

Cada una de las fases del proyecto nos aportó no sólo una manera de alcanzar los objetivos que nos planteamos, sino también una experiencia muy valiosa en el desarrollo de nuestra profesión.

Las bases para afianzar nuestros propósitos no se limitaron a los conocimientos adquiridos a lo largo de nuestra formación profesional. La investigación previa nos permitió plantear el entorno y las bases de nuestras pruebas, además de ahondar en puntos finos que complementan temáticas ya conocidas y abordar nuevas problemáticas.

Por otro lado, al conocer más profundamente las metodologías de auditoría de seguridad existentes y elegir el concepto de *pentesting*, pudimos acercarnos a un gran número de herramientas técnicas, explorar sus funcionalidades, sus ventajas, y sus limitantes. Lo anterior no sólo nos permite percibir la manera en que las vulnerabilidades son explotadas, sino que también nos coloca en una mejor posición para prevenir los posibles ataques informáticos a los que nos enfrentemos en el futuro.

La ejecución de nuestras pruebas fue la culminación de una planeación concebida desde las investigaciones previas y la consolidación de conocimientos, hasta la adaptación y seguimiento de procesos propios de una auditoría de seguridad que, en última instancia, nos permitió plasmar por escrito nuestros descubrimientos, nuestras propuestas y la viabilidad de su aplicación.

Al analizar la gran cantidad de información obtenida pudimos apreciar varios posibles riesgos de seguridad con diversos niveles de importancia en la infraestructura del laboratorio.

Para mitigar las vulnerabilidades identificadas, se realizaron varias propuestas, de entre las que destacan la actualización permanente de sistemas operativos y programas, monitoreo más estricto de las actividades que los usuarios llevan a cabo dentro de las instalaciones, así como de la cantidad de información que es divulgada por diversos medios, el cifrado de algunos canales de comunicación y la protección de cuentas y contraseñas.

Recapitulando, el interés de las empresas que encargan este tipo de trabajos a compañías especializadas se centra en descubrir sus huecos de seguridad, qué tan viable es el explotarlos, y qué impacto tendría en la empresa en caso de que algún ataque la vulnerara. Si tomamos esto en cuenta, si suponemos que el laboratorio toma el lugar de la empresa contratante y si revisamos los resultados generados, puede observarse que los beneficios esperados señalados al inicio de la tesis fueron completados puesto que se descubrieron huecos de seguridad reales que comprometían en mayor o menor medida la integridad del laboratorio y pudieron ser implementadas soluciones que robustecieron las medidas de

seguridad ya consideradas anteriormente, lo que se traducirá en mejor desempeño de las funcionalidades del laboratorio y en la reducción de posibilidades que se genere una eventualidad en el mismo.