

## Resumen

Los sistemas de seguridad se encargan del análisis de las vulnerabilidades de una red de comunicaciones y sus posibles soluciones, con el fin de preservar la confidencialidad, integridad, disponibilidad y uso legítimo del sistema de información. Por consiguiente, una red de comunicaciones se considera segura siempre y cuando todos los procesos se realicen bajo reglas y políticas establecidas por el sistema de seguridad.

Recientemente se ha oído hablar de una tecnología inalámbrica usada para la identificación y rastreo de objetos, denominada RFID (*Radio Frequency Identification*). En esta tecnología la información que caracteriza a un objeto está almacenada en etiquetas. Dichas etiquetas proporcionan la información cuando un lector, que se encuentra en las cercanías, realiza la petición a través de la generación de campos electromagnéticos.

Al utilizar el aire como medio de acceso, se presentan amenazas a la seguridad del sistema debido a que la información que se transmite puede ser interceptada por cualquier usuario. Dichas amenazas se centralizan en la lectura no autorizada de la información que almacena una etiqueta y en el acceso no autorizado a sistemas restringidos. Una violación de la seguridad repercute directamente en la calidad del servicio proporcionado a los usuarios del sistema, debido a que no se pueden garantizar las condiciones de operación establecidas en las políticas de servicio.

La presente tesis surge de la necesidad por tratar de neutralizar las amenazas a la seguridad presentes en redes RFID. Se estudiaron los sistemas RFID, a fin de incorporar



---

una capa de seguridad basada en algoritmos de autenticación de usuarios y cifrado de la información. Dicha capa se implementó físicamente usando VHDL (*Very high speed integrated circuit Hardware Description Language*) como lenguaje de descripción de hardware en dispositivos FPGA (*Field-Programmable Gate Array*), con su respectiva interfaz aérea.

Después de realizar pruebas de operación e intentos de intrusión al sistema, tales como la presencia de lectores y etiquetas no autorizados, se demostró la robustez de la capa de seguridad. Es muy importante señalar que el diseño de la capa de seguridad está apegado a las limitaciones en recursos de hardware de las etiquetas; pues éstas deben tener un costo de fabricación muy bajo, a fin de poder incorporarlas a cualquier objeto y hacer de RFID una tecnología base para las redes de nueva generación, en las que la conectividad con cualquier dispositivo es una característica clave.

