# CAPÍTULO 1: INTRODUCCIÓN

Este capítulo presenta un panorama general del problema de seguridad en redes de computadoras. Se presenta la utilidad de los sistemas de detección de intrusos y el cómo éstos se relacionan con el objetivo y organización del proyecto de tesis.

## 1.1 ANTECEDENTES

El panorama global que justifica la existencia de sistemas de detección de intrusos es muy importante. Las comunicaciones son una parte fundamental del desarrollo del mundo actual y su importancia en ámbitos económicos, científicos y privados es difícilmente negada debido al grado de dependencia que todo aspecto de la vida humana ha adquirido con esta comunicación rápida, sencilla y segura.

La mayor red que existe en la actualidad, accesible para todo aquel que desee formar parte de ella, es evidentemente Internet. El solo tamaño de este sistema hace que la probabilidad de experimentar una brecha de seguridad que ponga en riesgo el propio equipo aumente considerablemente cada año. De manera comercial, existen diversos tipos de *software* especializado en mejorar la seguridad de todo usuario que sea partícipe de una red de computadoras. Este tipo de programas son efectivos sólo hasta cierto punto, pero son insuficientes para detener todos los tipos de ataques que pueden presentarse al utilizar el sistema [4].

Desafortunadamente, el desarrollo exponencial de medios de comunicación y diferentes tecnologías cuya cumbre hasta el momento sigue siendo la gran red que conecta al mundo, Internet, también ha creado las circunstancias propicias para que aquellos que deseen obtener información de manera ilícita para sus fines propios puedan hacerlo interceptando, modificando y corrompiendo la información que es mandada o almacenada por las computadoras conectadas a una red. Es por esto que el concepto de

seguridad haya adquirido tanta importancia en los últimos años. Nunca se sabe quién intentará atacar o cómo lo hará.

## 1.2 PLANTEAMIENTO DEL PROBLEMA

Los sistemas destinados a resolver el problema de seguridad en la red son denominados IDS, *Intruder Detection Systems* o Sistemas de Detección de Intrusos por sus siglas en inglés. Estos sistemas analizan información que proviene del flujo de datos en una red computacional, la recolectan y clasifican para posteriormente generar una salida de acuerdo a su análisis.

Esta tesis será desarrollada como una opción en términos de IDS, creando un sistema capaz de reconocer ataques a una red computacional después de haber sido entrenado para hacerlo. El entrenamiento se basará en reconocimiento de patrones considerados normales para poder extender la respuesta del sistema a nuevas entradas, posibles amenazas, y para poder obtener una respuesta que permita tomar la acción correctiva adecuada [1].

Tanto los datos de entrenamiento como los datos de prueba estarán basados en comandos reales característicos de protocolo HTTP, los cuales tendrán por fin verificar que el sistema de detección sea en efecto capaz de predecir, generalizar y aprender a distinguir comandos peligrosos procedentes de ataques externos hechos por intrusos en la red de los comandos normales que caracterizan la operación de sistemas basados en este tipo de protocolo. El IDS estará entonces listo para ser añadido como elemento de seguridad a cualquier red que se necesite.

El esquema general de un IDS y su contexto dentro de una red se muestra en la Figura 1.1:

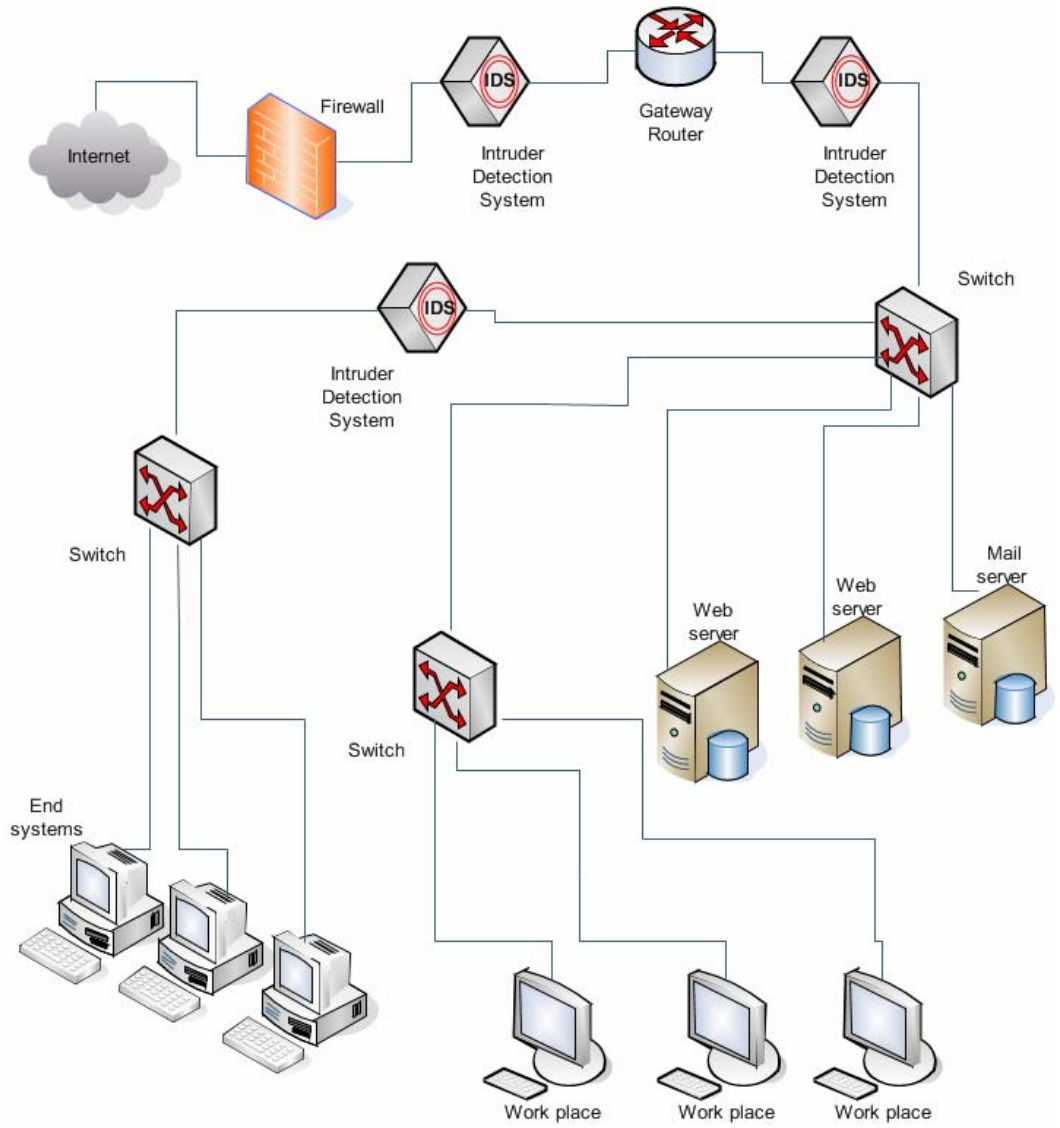


**Figura 1.1** Estructura de una red con sistemas de detección de intrusos

Los resultados del desarrollo de métodos para detectar intrusos en redes de computadoras han generado varias formas de abordar el problema. La principal es aquella en la que el sistema se enfoca a detectar comportamiento anómalo dentro de la red. Este enfoque tiene la ventaja de que el detectar anomalías es una forma más confiable de saber si hay un intruso en la red, ya que éste será el que genere comandos

anómalos o flujo de datos fuera de lo común. El problema es que un sistema que detecte intrusos de manera óptima debe saber reconocer ataques nuevos que nunca antes se hayan visto, por lo que debe ser capaz de aprender y generalizar.

Es por esto que se han seleccionado las redes neuronales como la herramienta más indicada para realizar esta tarea. Estas redes son capaces de responder a nuevos ataques, de aprender por sí mismas y de ser entrenadas para reconocer patrones normales y anormales, clasificándolos como se deseen. No obstante, las redes neuronales deben ser capaces de actualizarse en tiempo real para ser verdaderamente útiles como un IDS, y es por eso que esta tesis desarrollará una red neuronal recurrente (RNN) capaz de actualizarse a sí misma en tiempo real.

Como base utilizaremos una tesis anterior que desarrolló dos tipos de redes neuronales conocidas como *feedforward* y Elman [6] y mejoraremos dichas redes para obtener una RNN funcional por medio de simulación que nos permita comparar el desempeño de ambas. [3,5] La viabilidad del proyecto es alta en términos de prueba, simulación y diseño. Su implementación real, sin embargo, depende en gran medida del sistema de redes computacionales donde se desee utilizarlo y la cooperación de los administradores de dicho sistema.

Al tener el IDS en operación basado en redes neuronales, será posible entrenarlo para reconocer patrones inofensivos de patrones peligrosos en casi cualquier aplicación que deseemos. El único procedimiento que debe llevarse a cabo en ese caso es el preprocesado de datos que, tal como las rutinas de preprocesado desarrolladas en esta tesis, deberá preparar la información de manera que pueda ser entendida por la red; en este caso, que sea un archivo de caracteres binarios directamente relacionados con la información relevante. Esta característica de este sistema lo hace altamente adaptable y versátil en términos de aplicación.

## 1.3 OBJETIVO DE LA TESIS

El objetivo de esta tesis es modelar y simular un sistema de redes neuronales recurrentes capaz de trabajar en tiempo real para responder adecuadamente a ataques nuevos o no identificados a una red de computadoras, proporcionando información suficiente que permita tomar una acción correctiva, para comparar el desempeño de dicha red neuronal con una tipo *feedforward* y llegar a una conclusión acerca de la efectividad de la primera.

Esperamos que el IDS basado en RNN tenga un desempeño superior a aquellos basados en redes *feedforward* y Elman, y con estos resultados comprobar que el tipo de arquitectura y organización así como los algoritmos de aprendizaje de las redes neuronales recurrentes les permite arrojar mejores resultados en cuanto a efectividad y porcentaje de error se refiere.

## 1.4 ORGANIZACIÓN DE LA TESIS

La tesis está organizada en siete capítulos y dos apéndices, los cuales describen el proyecto en su totalidad.

Se enumerarán los tipos de sistemas en los que dichos dispositivos son utilizables y se discutirá su relación con los ataques basados en el protocolo HTTP en el capítulo dos. Los diferentes tipos de ataques y sus efectos potenciales considerados para esta tesis recibirán atención especial.

También se enumerarán las diferentes clases de redes neuronales en el capítulo tres con énfasis especial en las redes neuronales recurrentes (RNN). En particular, se considerarán las ventajas y desventajas que hacen a éstas mejores a los otros dos tipos de redes consideradas.

En el capítulo cuatro se describirán a detalle los algoritmos de aprendizaje que coordinan el desempeño de las redes neuronales. Mediante estos algoritmos es que las redes aprenderán y asimilarán los datos de entrada para poder ser probadas con datos nuevos en el IDS.

En el capítulo cinco se dará una descripción detallada del modelado y la simulación del IDS con redes neuronales en sus tres variaciones diferentes. Se explicarán las razones por las que las redes neuronales fueron diseñadas con las características específicas que al final obtuvieron.

Las pruebas hechas con el IDS basado en RNN y la comparación de los resultados con los de las redes *feedforward* y Elman para verificar si el desempeño de las primeras es superior, respectivamente, se verá en el capítulo 6. También se demostrará que las RNN son mejores que las otras dos.

En el capítulo siete estos resultados serán la base de las conclusiones y el posible trabajo a futuro como continuación de la presente tesis. Se evaluarán las características positivas y negativas de la propuesta de solución al problema de desarrollar un IDS eficiente desde el punto de vista de las RNN.

Se incluyen asimismo dos apéndices con el código fuente del IDS, la explicación y comentarios pertinentes (Apéndice A) y los datos utilizados para la realización del programa (Apéndice B). Ambos apéndices pueden ser encontrados también en el CD adjunto a este documento.