Métodos estadísticos aplicados a ciberseguridad

Introducción

La ciberseguridad es el conjunto de prácticas específicamente diseñadas para la protección de las redes computacionales y todos los elementos que las conforman de ataques maliciosos. Actualmente, la ciberseguridad es un tema de suma importancia y uno de lo grandes desafíos al que nos enfrentamos como individuos y como sociedad. Es por ello que la ciberseguridad requiere de un esfuerzo multidisciplinario, siendo la estadística una pieza fundamental para el análisis y la detección de los diferentes tipos de ciberataques.

Objetivo

El objetivo de este curso es exhibir la importancia, las ventajas, los retos y las áreas de oportunidad de la estadística aplicada a la ciberseguridad. Para ello, nos centraremos en el estudio de tres clases de ciberataques, para los cuales se proveerá la terminología y el contexto general que servirán como bases para la correcta comprensión de los datos, los supuestos y los diferentes enfoques y modelos estadísticos que han sido utilizados para su detección. Al ser un curso introductorio, no nos adentraremos en el desarrollo matemático riguroso de los modelos, sino en su comprensión, su planteamiento y su uso general dentro de la ciberseguridad.

Temario

Introducción

- Orígenes de la ciberseguridad
- Modelo de referencia OSI
- Monitoreo y análisis de una red

Análisis y detección de anomalías en el volumen de tráfico

- Introducción a los modelos de punto de cambio
- Enfoque sequencial y detección a tiempo real
- Aplicación a ciberseguridad

Detección de anomalías en la red

- Análisis de las conexiones de una red computacional
- Modelado de nuevas conexiones

Malware

- Definición y variedades
- Análisis estático de malware
- Análisis dinámico de malware

Otras clases de anomalías

- Spam
- Phishing
- Anomalías en sistemas de cómputo distribuidos