


# Instituto Tecnológico De Cancún

**Materia:**

Fundamento De Telecomunicación

**Titulo:**

Investigar sobre SIEM e IDS/IPS

Tun Cauich Alejandra Noemi

**Turno:** 5:00 a 6:00. P.M

**Docente:**

ING.ISMAEL JIMÉNEZ SÁNCHEZ

SIEM e IDS/IPS

Although the three tools are used to monitor and detect intrusions in the company's computers or network, they are different from each other. Next, we describe each one of them.

IDS
IDS (Intrusion Detection System) or intrusion detection system: it is an application used to detect unauthorized access to a computer or a network, that is, they are systems that monitor incoming traffic and check it against an updated database of firm known attack numbers. In the event of any suspicious activity, they issue an alert to the system administrators who must take the appropriate measures. These accesses can be sporadic attacks carried out by malicious users or repeated from time to time, launched with automatic tools. These systems only detect suspicious accesses by issuing anticipatory alerts of possible intrusions, but they do not try to mitigate the intrusion. His performance is reactive.

IPS
IPS (Intrusion Prevention System) or intrusion prevention system: is a software used to protect systems from attacks and intrusions. Its action is preventive. These systems carry out a real-time analysis of the connections and protocols to determine if an incident is occurring or will occur, identifying attacks based on patterns, anomalies, or suspected behaviors attacking desos and permitted policies that are based on the content of the monitored traffic, that is, the IPS in addition to triggering alarms, can discard packets and disconnect connections.

Many providers offer mixed products, calling them IPS / IDS, frequently integrating with firewalls and UTM (in English Unified Threat Management or Unified Threat Management) that control access based on rules on protocols and on the destination.

SIEM
SIEM (Security Information and Event Management) or security information and event management system: it is a centralized hybrid solution that encompasses the management of security information (Security Information Management) and the management of events (Security Event Manager). SIEM technology provides real-time analysis of security alerts generated by different hardware and software devices on the network. It collects the activity records (logs) of the different systems, relates them and detects security events, that is, suspicious or unexpected activities that can lead to the start of an incident, discarding anomalous results, also known as false positives, and generating responses based on the reports and evaluations that it records, that is, it is a tool in which the information is centralized and is integrated with other threat detection tools.