

**FACULTAD DE INGENIERÍA:**

**CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

**TITULO:**

TAREA SESIÓN 10

**INTEGRANTES:**

YAYA PURIZACA, MANUEL ALEJANDRO

**CURSO:**

SEGURIDAD INFORMÁTICA

Piura - Perú

2024

1. **¿*Cómo se debería implementar un IPS?* Brinda un ejemplo.**

Si se elige entre un **NIPS** o un **WIPS**, el IPS se implementa entre el tráfico entrante y el cortafuegos o el **gateway** de la red. El IPS analizará el tráfico de la red para detectar patrones de ataque y tomar acciones correctivas cuando sea necesario.

Si se opta por un **HIPS**, el IPS se instalaría en cada dispositivo individual (servidor, estación de trabajo, laptop) para monitorizar las actividades locales, como la ejecución de procesos o la manipulación de archivos.

Un IPS requiere que se configuren políticas de seguridad detalladas. Estas políticas definen qué tipos de tráfico son permitidos, qué actividades son consideradas sospechosas o maliciosas y qué acciones debe tomar el IPS ante un evento de seguridad (por ejemplo, bloquear el tráfico, terminar una sesión, generar una alerta, etc.).

* Las **firmas de intrusión** también deben ser configuradas o actualizadas. Estas son las definiciones de patrones de ataques conocidos que el IPS busca en el tráfico de red.
* Las **políticas de acceso** y **listas de control** definen qué dispositivos o usuarios pueden acceder a ciertos recursos, lo cual es crucial para la integración con tecnologías como las VPN.

**5. Monitoreo y Respuesta a Incidentes**

Una vez implementado, el IPS debe ser monitorizado de forma continua. Las alertas generadas por el IPS deben ser analizadas por el equipo de seguridad para determinar si la amenaza es real y cómo responder.

Además, se deben revisar los registros del IPS (y del firewall, si se usa) para realizar auditorías y análisis forenses en caso de un incidente de seguridad.