Curso de Monitorización de la seguridad

Escenarios, existen cuatro tipos

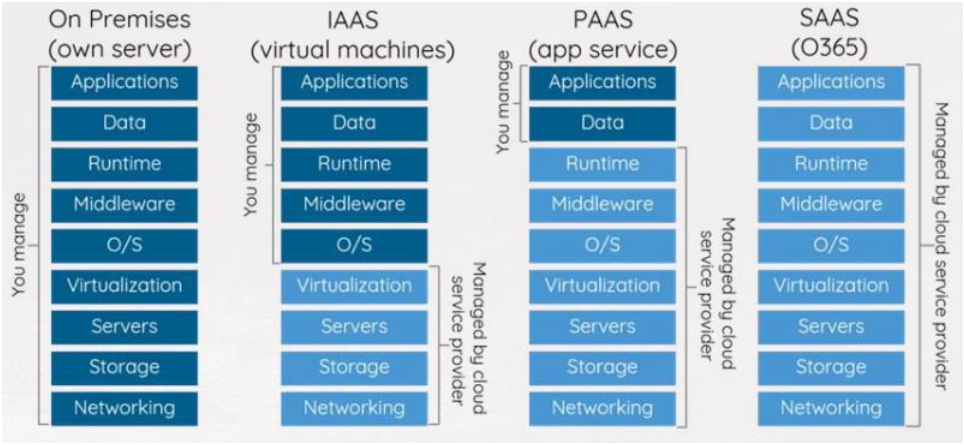
- Centros de procesos de datos, los cuales suelen ser un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento informático y electrónico, suelen ser creados y mantenidos por grandes organizaciones.

Los factores que llevan a la creación de CPD son: garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras.

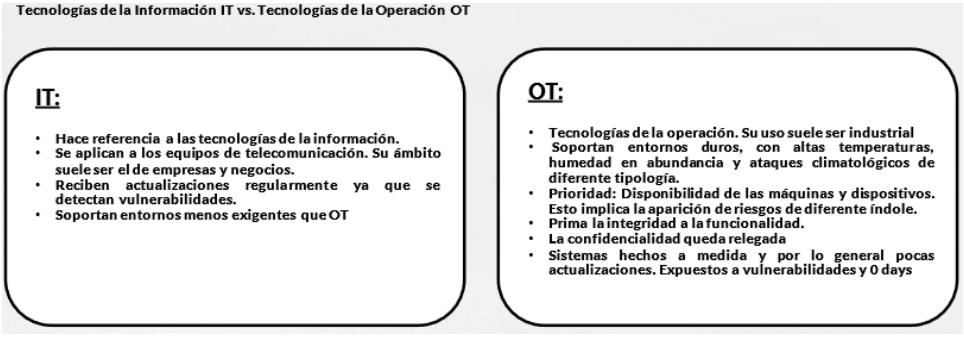
- Virtualización, se basa en la creación de máquinas virtuales a partir de una única máquina física. Se compone de tres componentes principalmente, hipervisor (VMware, VirtualBox), el host (máquina física sobre la que se crean las virtuales) y la máquina virtual

  Optamos por la virtualización ya que tiene ciertas ventajas como que es más económico puesto que se reduce el uso de hardware y el consumo de electricidad, es más seguro ya que hay menos componentes físicos, además los backups son más sencillos.

- La nube, se basa en la utilización de recursos (servidores, almacenamiento, capacidad de cómputo) que se encuentran en internet. La gestión de dicha infraestructura es responsabilidad de un tercero, también busca optimizar la infraestructura mediante la automatización para conseguir una flexibilidad y adaptabilidad de los recursos.
  Una organización puede usar esos recursos para montar servicios de forma eficiente.
  El objetivo de la nube es la disminución de los costes puesto que no se necesita una infraestructura, se busca la escalabilidad ya que podemos acceder a los recursos de manera casi instantánea, la flexibilidad, ya que se pueden aumentar puntualmente los recurso si se produce un pico de uso, y una gran disponibilidad.
  Existen varias modalidades que en orden de menor a mayor dependencia IAAS, PAAS, SAAS

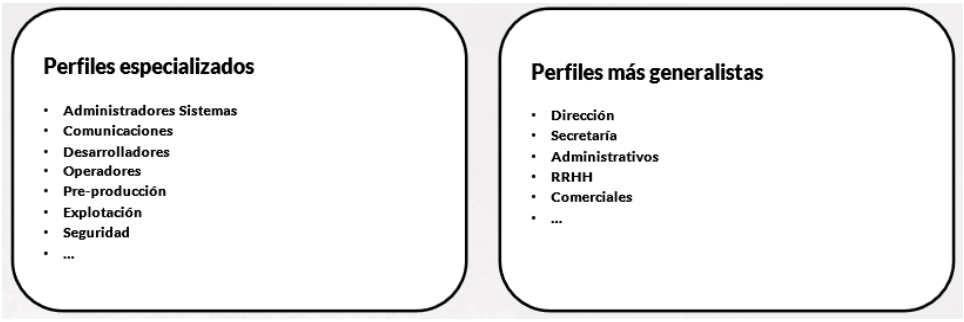


- Entornos OT



Actores

Son todas las personas que tienen acceso a la información, los podemos dividir en dos grupos especializados y generalistas



Atacantes

Los atacantes suelen hacer uso de distintos frameworks que facilitan su tarea, algunas de las herramientas más comunes son:

Kali Linux que incluye herramientas, para Ingeniería social, buscadores y OSINT

Social Engineer Toolkit que está orientada a la ingeniería social, phising, robo de credenciales...

Google hacking que se basa en una búsqueda más específica y entrar en archivos como el robots.txt para descubrir posibles vulnerabilidades

Defensa

Los métodos usados para la defensa son herramientas de protección perimetral como firewall o proxys, controles de usuarios, SOAR

Para monitorizar todo esto se utiliza SIEM que es una herramienta que nos permite analizar y comparar los datos obtenidos con otras fuentes como pueden ser bases de datos.

Con herramientas como MITRE podemos ver el estándar para cada una de las fases del Cyber Kill Chain que son todas las fases por las que pasa el atacante para realizar su ataque.

Con el uso de TIP podremos recolectar información sobre inteligencia sobre amenazas

Con el uso de SOAR podemos gestionar vulnerabilidades y amenaza, generar una respuesta ante incidentes, y generar una automatización para responder de manera automática n el futuro