Clase 2: Conceptos básicos de ciberseguridad (Continuación)

Elementos de seguridad física

La seguridad física se refiera a **medidas y estrategias implementadas para proteger activos físicos**, personas e instalaciones de acceso no autorizado, daño y robo.

La seguridad física **complementa las medid de ciberseguridad** para proveer protección contra las amenazas.

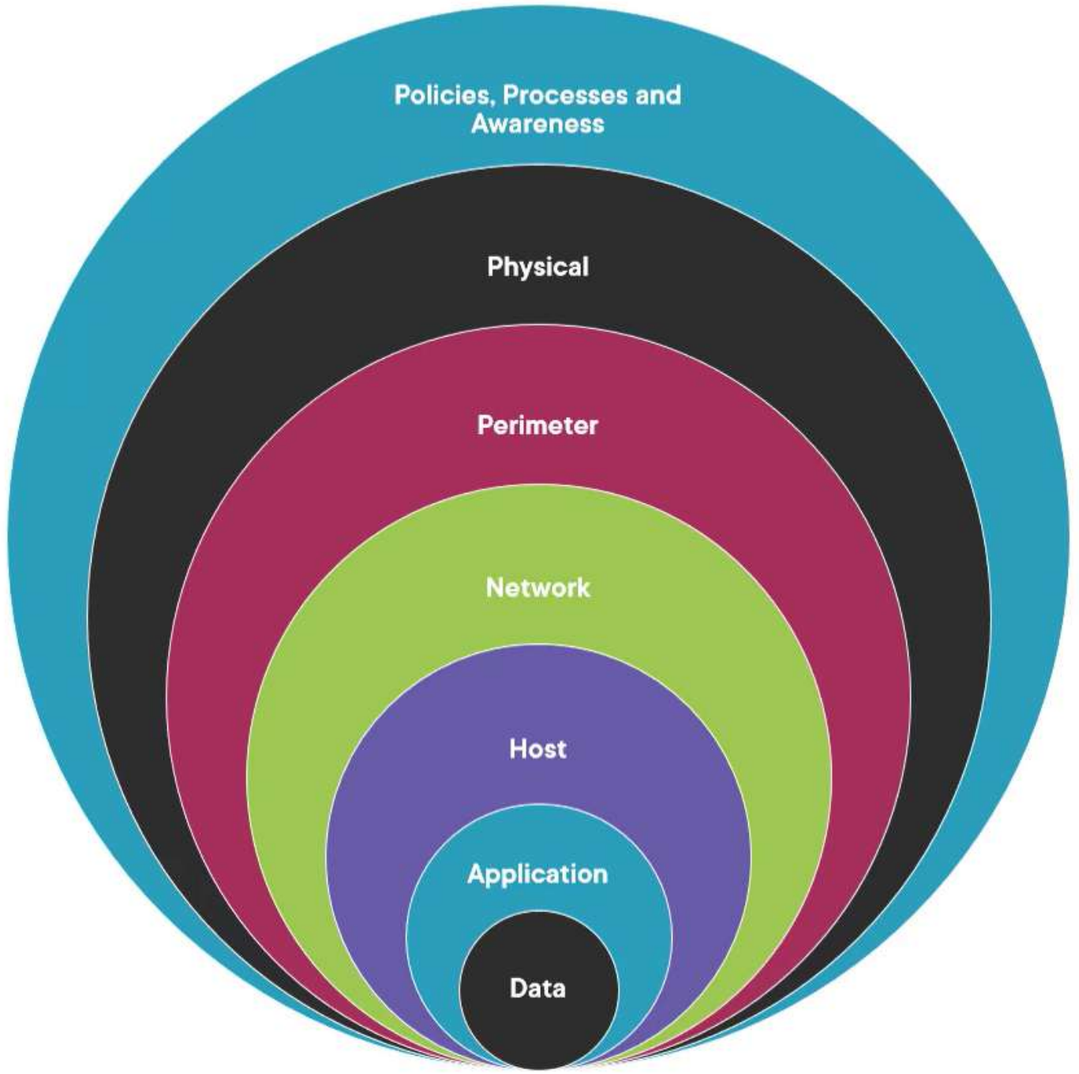
Control de entendimiento

¿Los controles de seguridad sirven para proteger las a los miembros del departamento de ventas?

Verdadero

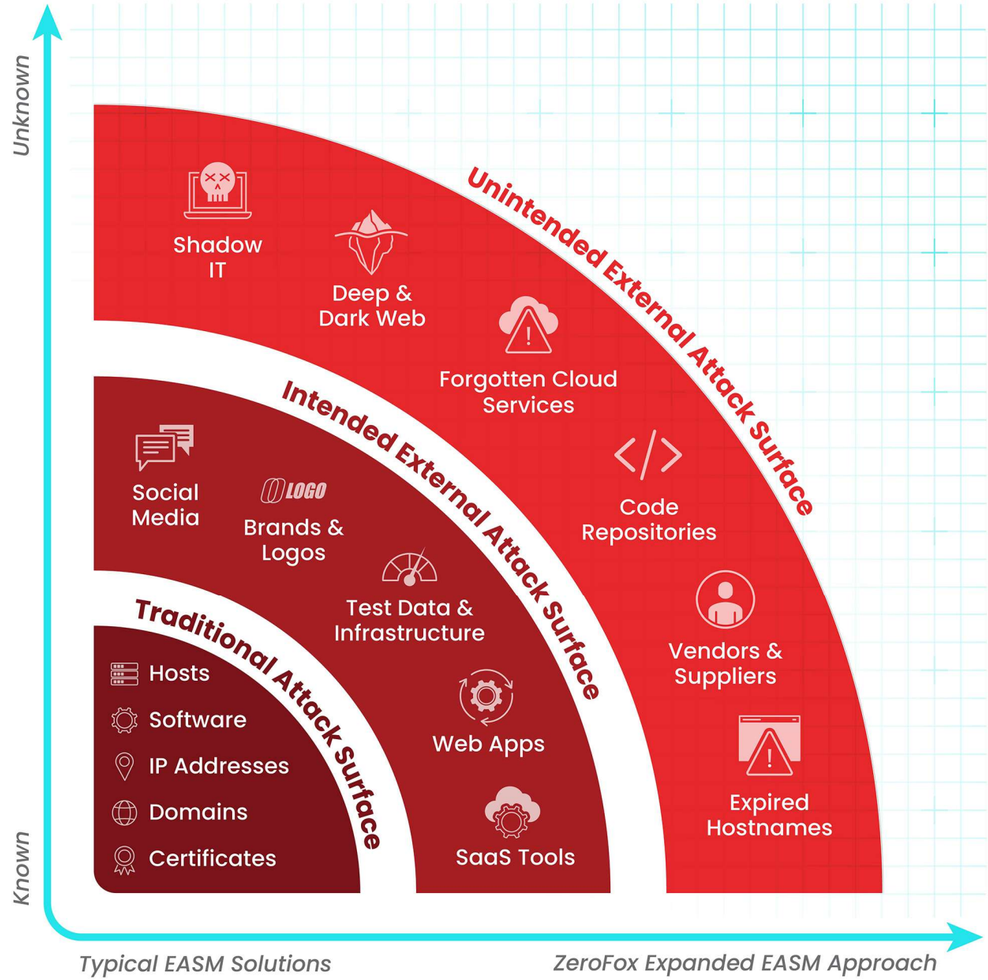
Defensa en profundidad (Defense in Depth)

- Defensa/Seguridad por capas
- Siempre se debe pensar "¿qué pasaría si este control de seguridad es traspasado?"
- Controles de seguridad de distintas categorías y distintos tipos



Defensa en profundidad (Defense in Depth)

- El propósito es **no** tener un "**único punto de falla**" (single point of failure)
- Zero Trust
- Nunca ignorar la seguridad perimetral



Control de entendimiento

¿La seguridad por capas sirve para proteger un activo solamente, al instalarle varias soluciones de seguridad?

Falso

Control de entendimiento

¿El “único punto de falla” es cuando una organización solamente tiene una única solución de seguridad?

Verdadero

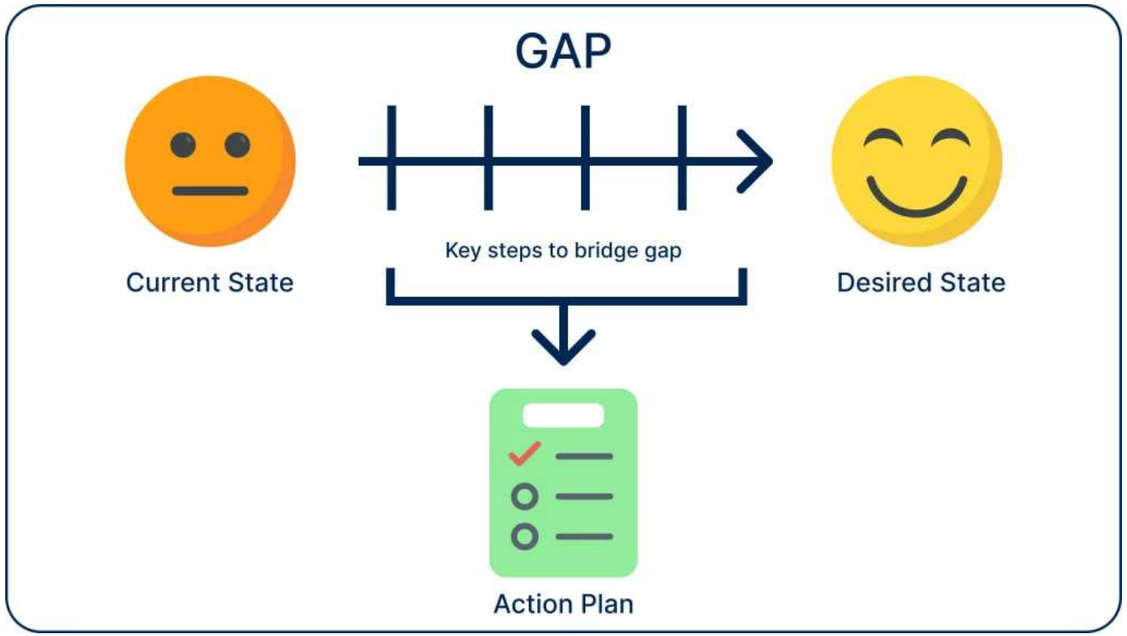
Análisis de brecha (Gap analysis)

Es una herrramienta usada para evaluar la variación/brecha entre el estado actual y el nivel deseado de procesos, sistemas, organización o proyectos.

Compara prácticas, rendimiento o capacidades existentes contra criterios, estándares u objetivos predefinidos.

Identifica areas donde falla el estado actual.

Ayuda a priorizar mejoras y desarrollar planes de acción para solventar la brecha.



Análisis de brecha (Gap analysis)

El análisis de brecha es crucial para identificar oportunidades de:

- Crecimiento
- Opminización de rendimiento
- Conseguir objetivos estratégicos

Ejemplo práctico:
Se requiere identificar la exposición de la superficie de ataque de la empresa. Posibles resultados:

- Ubicaciones expuestas a ataques
- Poca o nula intervención directa
- Centrarse en educación

Los resultados del ejemplo no son los únicos que se pueden dar. Son solo ejemplos.

Control de entendimiento

¿La “brecha” en el análisis de brechas se refiere a qué tan vulnerable es un sistema?

Falso

Control de entendimiento

¿El análisis de brechas evalúa el estado actual de un sistema comparándolo con el estado deseado?

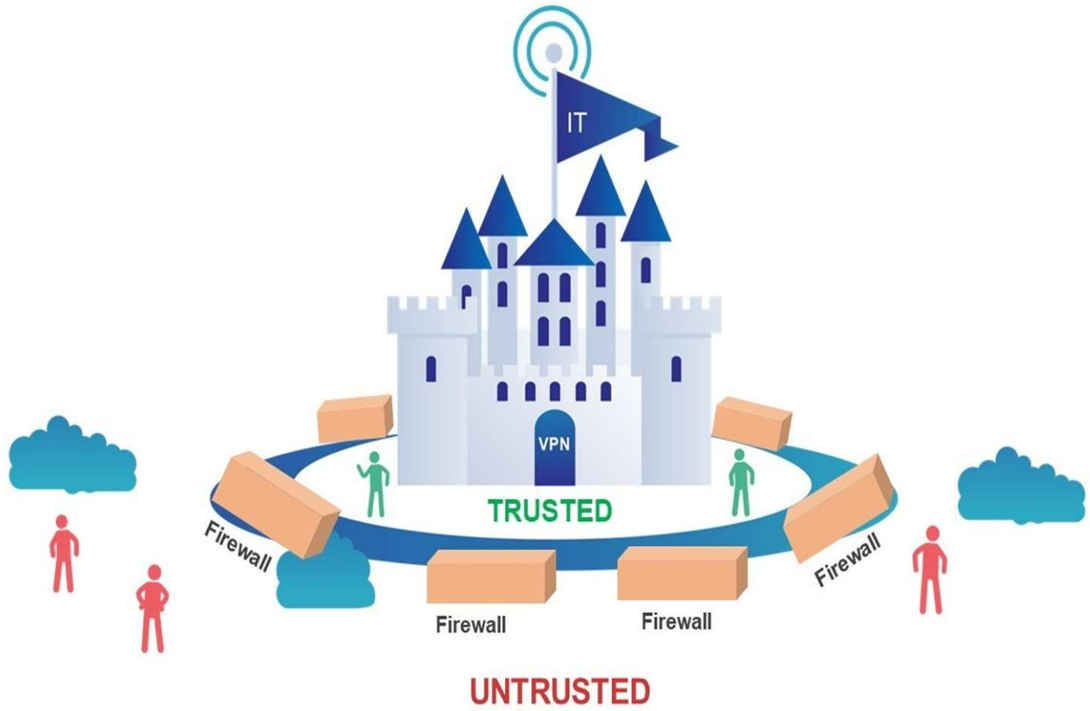
Verdadero

Arquitectura Zero Trust (Cero Confianza)

Es un marco de trabajo de ciberseguridad que opera bajo el principio de nunca confiar, siempre verificar.

Este framework asume que las amenazas pueden existir tanto fuera como dentro de una red; por ello, no se debe confiar por defecto en ninguna entidad.

Controles y medidas de seguridad se implementan basadas en validación estricta de identidad, monitoreo continuo, y principio de mínimo privilegio.



Arquitectura Zero Trust – Plano de control

Usado para gestionar y aplicar centralmente políticas de seguridad en la red, aplicaciones y recursos de una organización.

- Identidad adaptable: involucra **evaluar continuamente** identidades de usuarios, sus acciones y el contexto exacto de sus intentos de acceso para **brindar o bloquear su acceso**.

- Reducción de alcance de amenaza: se refiere a la práctica de segmentar la red e implementar controles de acceso estrictos **para limitar el impacto de brechas de seguridad**.

- Control de acceso dirigido por políticas: aplica **controles de acceso basados en políticas** de acceso predefinidas en lugar de confiar solamente en los perímetros de red o confianza asumida.

- Motor de políticas: **toma las decisiones** de acceso y las registra.

- Administrador de políticas: **ejecuta las decisiones** del motor de políticas.

Arquitectura Zero Trust – Plano de datos

Usado para facilitar la transmisión y procesamiento de datos de manera segura.

- Zonas implícitas de confianza: se refiere a **segmentos lógicos o físicos** de una red que tienen seguridad mejorada para proteger **activos sensibles**.

- Sujeto/Sistema:
  - "sujeto" es la entidad que **busca obtener acceso** (usuario, dispositivo, aplicación...);
  - "sistema" es la infraestructura, aplicación, datos o servicio **al que un sujeto quiere acceder**.

- Punto de cumplimiento de políticas: sirve para habilitar, monitorear y eventualmente terminar las conexiones entre un sujeto y un recurso.

Control de entendimiento

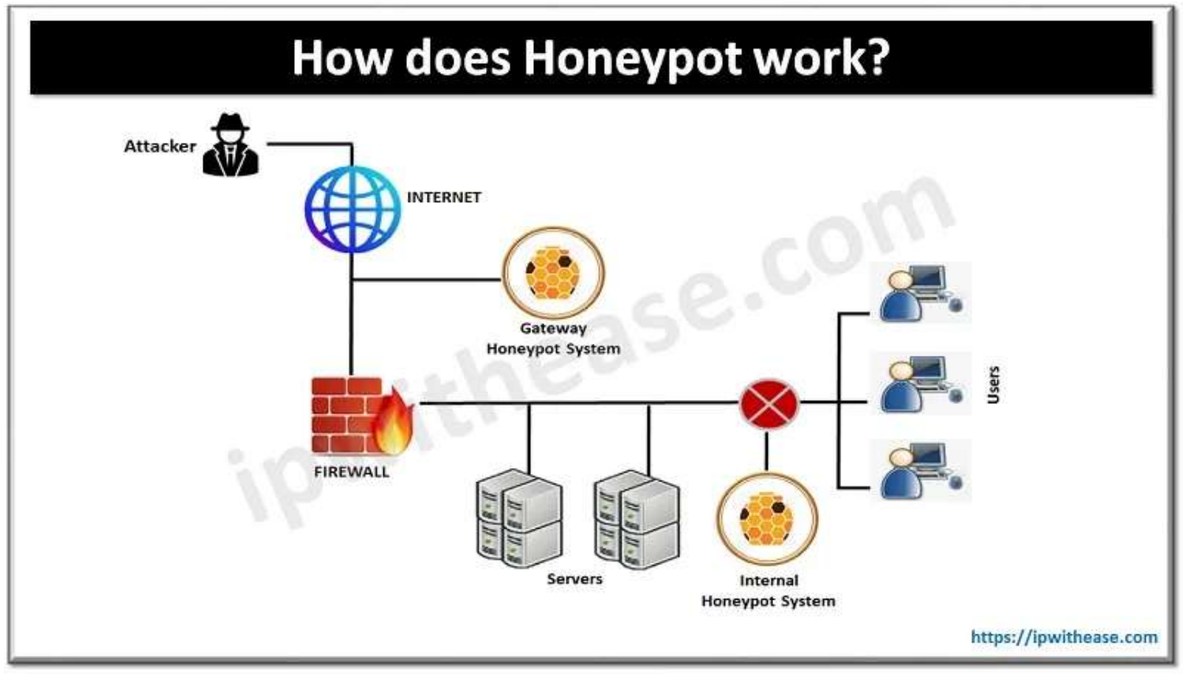
¿El framework zero trust se llama así porque se sugiere que “nunca confíes en nadie, ni siquiera en tus héroes”?

Falso

Engaño e irrupción tecnológica

Un **honeypot** (bote de miel) es un sistema configurado para **simular uno o varios servicios en la organización**, con el objetivo de servir de señuelo para que un **atacante intente explotarlo** y así registrar su actividad de manera segura para su futuro análisis.

- Una **honeynet** es un conjunto de honeypots.
- Un **honeyfile** es un archivo que sirve como señuelo.
- Un **honeytoken** es un archivo que contiene un token de rastreo (por si se obtiene acceso al equipo del atacante).



Control de entendimiento

¿Un honeypot sirve para engañar a un atacante haciéndolo pensar que está dentro de la red de la organización?

Verdadero

Control de entendimiento

Práctica

En TryHackMe

Procesos de negocios que afectan las operaciones de seguridad

Proceso de aprobación: aseguran que cualquier cambio pase primero por una revisión y autorización por los interesados (stakeholders), reduciendo el riesgo de generar vulnerabilidades.

Propiedad: asignar a un individuo o equipo la responsabilidad de gestionar y vigilar un cambio, asegurando el registro y un claro punto de contacto.

Stakeholders: son los individuos afectados por un cambio. Sus inversiones son cruciales para implementar el cambio con éxito.

Análisis de impacto: evalúa los efectos potenciales efectos de los cambios propuestos en las operaciones, seguridad, y sistemas.

Resultados de pruebas: proveen evidencias de que un cambio funcionará como se espera sin comprometer la seguridad, identificando problemas antes de la implementación.

Plan de retroceso: estrategia predefinida para revertir rápidamente un cambio si este causa problemas inesperados o de seguridad.

Procesos de negocios que afectan las operaciones de seguridad

Ventana de mantenimiento: es un periodo calendarizado/agendado durante el cual se implementan los cambios, típicamente escogidos para minimizar el impacto en las operaciones y reducir el riesgo de incidentes de seguridad durante el proceso.

Procedimiento operacional estándar (SOP): instrucciones paso por paso que detallan el proceso y las buenas prácticas para implementar un cambio, asegurando consistencia, cumplimiento y seguridad a lo largo de la organización.

Control de entendimiento

¿El análisis de impacto permite evaluar los efectos que tendrá un cambio al ser implementado?

Verdadero

Implicaciones técnicas de los cambios

Listas de permitidos/denegados: permiten o niegan el acceso a entidades o aplicaciones específicas. Deben manejarse con cuidado para no generar DoS.

Actividades restringidas: aquellas a las cuales se tiene acceso limitado o prohibido, con el fin de proteger la seguridad e integridad de sistemas y datos.

Tiempo de inactividad: periodo en el cual un sistema no se encuentra debido a mantenimiento, actualizaciones o problemas inesperados, impactando las operaciones y exponiendo sistemas a posibles vulnerabilidades de seguridad.

Reinicio de servicios: detener e iniciar un servicio para aplicar cambios, lo que puede generar una interrupción pero a la vez es necesario.

Implicaciones técnicas de los cambios

Reinicio de aplicación: cerrar y abrir otra vez una aplicación para aplicar cambios, que podría crear interrupción de servicio y afectar la productividad del usuario.

Aplicaciones heredadas (legacy): son sistemas de software desactualizados que pueden no tener soporte o actualizaciones regulares, generando un riesgo debido a las vulnerabilidades potenciales y los problemas de compatibilidad.

Dependencias: interconexiones entre software, hardware y servicios diferentes, donde los cambios en un componente pueden impactar la funcionalidad y seguridad de otros.

Control de entendimiento

¿El reinicio de servicios puede causar denegación/interrupccón de servicios?

Verdadero

Control de entendimiento

¿Las listas de permitidos sirven más que las listas de denegados?

Dependeee