BASTIONADO DE REDES Y SISTEMAS

TEMA 1: INTRODUCCIÓN

CONCEPTO CLÁSICO

- El nombre Host bastión deriva de un término medieval que describe los muros de un castillo. Un bastión es un lugar especial, fortificado, de un muro defensivo diseñado especialmente para repeler ataques.
- Por tanto, en informática, un host bastión es un ordenador especialmente fortificado contra los ataques de red. Los diseñadores y administradores de red colocan estos ordenadores posicionados como primera línea de defensa, proporcionando así un punto de estrechamiento de todas las comunicaciones entre la red e Internet. En otras palabras, ningún ordenador de Internet puede acceder a la red sin pasar primero por aquí, lo que permite controlar con mucha facilidad la seguridad de la red y configurar adecuadamente los sistemas.

¿ QUÉ ES EL BASTIONADO (HARDENING) ?

- BOE:
- La función de bastionado incluye aspectos como la administración de los sistemas y redes contemplando la normativa, tanto a nivel nacional como internacional, de ciberseguridad en vigor.
- Las actividades profesionales asociadas a esta función se aplican en el diseño de planes de securización y en el diseño de las redes contemplando los requisitos de seguridad que apliquen a la organización.

¿ POR QUÉ ES IMPORTANTE EL HARDENING DE LOS SISTEMAS Y LAS REDES DE COMUNICACIÓN ?

- **Antes:** Las empresas estaban relativamente poco expuestas desde Internet, ya que la mayoría de sus gestiones las realizaban en formato papel o en equipos aislados.
- **Hoy:** Las empresas tienen prácticamente todos sus ámbitos conectados a Internet: inventariado, compras, página web, ventas al público, recursos humanos…

ACTORES QUE ENTRAN EN ESCENA

- **Ciberactivistas:**
  - Concienciados por una causa política o social.
  - No buscan fama ni dinero, pero sí castigar al objetivo.
- **Cibercriminales:**
  - Buscan enriquecimiento, pero no notoriedad.
- **Terroristas cibernéticos:**
  - Conocen el efecto negativo que tienen ciertas acciones informáticas.
- **Agentes estatales:**
  - Espías y servicios de inteligencia de otros países.

¿ CÓMO HA IDO EVOLUCIONANDO EL CONCEPTO DE CIBERSEGURIDAD ?

- **Antes**: La ciberseguridad se veía como un asunto técnico que se dejaba en manos de los expertos en TI que hubiera, pero poco más.
- **Ahora**: Se ha descubierto que se requiere una estrategia holística (que englobe todos los aspectos de la empresa), ya que la ciberseguridad conlleva riesgos:
  - Riesgos financieros.
  - Riesgo operacionales.

Y RECUERDA…

- Por muy seguras que sean las medidas, siempre habrá **alguien que logrará romperlas**, con el tiempo.
- El análisis de los riesgos (que se verá en el próximo tema con más profundidad) **es un proceso contínuo y holístico.**
- Al final, el eslabón más débil de la cadena siempre seremos **las personas.**

ACTIVIDAD 1

- Realizar la actividad de Moodle: Noticias sobre ciberataques
  - Se valorará:
    - Originalidad en los resultados.
  - Penaliza:
    - Copia-pega sin aportar nada nuevo ni explicar con tus propias palabras.

ACTIVIDAD 2

- Realizar la actividad de Moodle: Ciberataque a Maersk
  - Se valorará:
    - Contestar con tus propias palabras.
  - Penaliza:
    - Contestaciones escuetas.
    - Copiar-pegar.

ACTIVIDAD 3

- Realizar la actividad de Moodle: Medidas de seguridad obsoletas
  - Se valorará:
    - Identificar más de cinco fallas en temas de seguridad.
    - Explicar por qué es una falla y cómo se puede comprometer la seguridad del sistema.
  - Penaliza:
    - Contestaciones escuetas.