CURSO	
CURSO:	CIBERSEGURIDAD
CATEDRÁTICO:	LIC. BRENDA GALVAN
HORAS	3 HR

CURSO	EN LÍNEA
NÚMERO DE TELÉFONO (DUDAS)	
REGISTRARTE AQUÍ	SOLO 10 CUPOS

Sesión 1: Fundamentos y marco conceptual

1. **Introducción a la ciberseguridad**
   - **Definición y objetivos clave**
     - Confidencialidad: proteger la información contra accesos no autorizados.
     - Integridad: garantizar que los datos no sean alterados indebidamente.
     - Disponibilidad: asegurar el acceso a la información cuando sea necesario.
   - **Importancia en el entorno empresarial y personal**
     - Riesgos de no tener controles adecuados.
     - Beneficios de una buena estrategia de seguridad.
   - **Evolución histórica**
     - Hitos clave en la historia de la seguridad informática.
     - Incidentes que marcaron precedentes en el mundo digital.
2. **Componentes de un sistema seguro**
   - **Activos críticos**
     - Identificación de datos sensibles, aplicaciones y dispositivos.
   - **Roles y responsabilidades**
     - Función del usuario final, administrador de sistemas y equipo de seguridad.
   - **Aplicación de la triada CIA en la práctica**
     - Ejemplos concretos de cómo proteger activos en escenarios diarios.
3. **Normativas y buenas prácticas**
   - **Estándares internacionales**

- ISO/IEC 27001: sistema de gestión de seguridad de la información.
- NIST Cybersecurity Framework: pasos para implementar controles.

- **Políticas de seguridad**
  - Gestión de contraseñas: reglas y recomendaciones.
  - Backups periódicos: planificación y verificación de copias de seguridad.
- **Ciclo de vida de la seguridad**
  - Identificación → Protección → Detección → Respuesta → Recuperación.

Sesión 2: Amenazas y vulnerabilidades comunes

1. **Introducción a la sesión**
   - Objetivos: diferenciar los tipos de amenazas y comprender su funcionamiento.
2. **Malware y su funcionamiento**
   - **Clasificación principal**
     - Virus: programas que se replican al infectar archivos legítimos.
     - Troyanos: software camuflado que abre puertas traseras.
     - Gusanos: se propagan automáticamente a través de la red.
     - Ransomware: cifra datos y exige rescate para su liberación.
3. **Ingeniería social y técnicas de engaño**
   - **Phishing y spear phishing**
     - Características que los distinguen y señales de alerta.
   - **Vishing y smishing**
     - Fraudes a través de llamadas telefónicas y mensajes SMS.
   - **Pretexting y baiting**
     - Escenarios falsos para inducir al usuario a revelar información.
4. **Vulnerabilidades en software y hardware**
   - **Fallos de configuración**
     - Puertos innecesariamente abiertos, contraseñas por defecto.
   - **Vulnerabilidades de día cero y parches de seguridad**
     - Importancia de mantener los sistemas actualizados.
   - **Explotación en aplicaciones web**
     - Inyección SQL, Cross-Site Scripting (XSS) y otras técnicas comunes.
5. **Ataques de red más frecuentes**
   - Denegación de servicio distribuida (DDoS).
   - Man-in-the-Middle (MitM) y sniffing de tráfico.
   - Envenenamiento de ARP y suplantación de DHCP.
6. **Análisis de un caso práctico breve**
   - Descripción de una brecha de seguridad real:
     - Vulnerabilidad explotada.
     - Consecuencias y aprendizajes

Sesión 3: Estrategias y herramientas de protección

1. **Principios de defensa para usuarios**
    - **Gestión segura de contraseñas**
        - Creación de contraseñas robustas y uso de gestores.
    - **Autenticación Multifactor (MFA)**
        - Tipos de factores (SMS, apps de autenticación, tokens).
    - **Principio de privilegio mínimo**
        - Asignación de permisos justos y necesarios.
2. **Seguridad en redes y entornos internos**
    - **Firewall y control de tráfico**
        - Configuración básica para permitir o bloquear conexiones.
    - **IDS/IPS (Sistemas de detección y prevención de intrusiones)**
        - Funcionalidad y ejemplos de uso en la red.
    - **Segmentación de red con VLANs**
        - Aislamiento de recursos críticos para minimizar riesgos.
    - **VPN y cifrado de comunicaciones**
        - Uso de protocolos TLS/SSL para proteger datos en tránsito.
3. **Protección de endpoints y dispositivos móviles**
    - **Soluciones antivirus y EDR (Endpoint Detection and Response)**
        - Diferencias entre antivirus tradicionales y sistemas EDR.
    - **Políticas de Mobile Device Management (MDM)**
        - Normas para dispositivos personales (BYOD) en la empresa.
    - **Actualizaciones automáticas y parches**
        - Procedimientos recomendados para mantener equipos al día.
4. **Plan de respaldo y respuesta a incidentes**
    - **Estrategias de backup**
        - Copias locales, remotas y en la nube; pruebas periódicas de restauración.
    - **Pasos del plan de respuesta a incidentes**
        - Detección → Contención → Erradicación → Recuperación → Lecciones aprendidas.
    - **Comunicación interna y externa**
        - Roles clave: quién avisa a quién y qué canales se usan en caso de brecha.