Ciberseguridad Básica Tácticas y Herramientas

Portal BlueSky Financial

Modalidad Online

Duración: 2 horas

Certificación Digital

Objetivo General del Curso

- Comprender los riesgos digitales más comunes y aplicar medidas prácticas para proteger la información personal y corporativa.
- Aprender tácticas de protección ante phishing, malware y otros ataques.
- Implementar configuraciones seguras en cuentas, redes y dispositivos.

Módulos

Módulo 1 · Fundamentos de Ciberseguridad

Módulo 2 · Cuentas y dispositivos Seguros

Módulo 3 · Redes y protección de datos

Módulo 4 · Respuestas Básica e indicadores

Módulo 1: Fundamentos de Ciberseguridad

- Conceptos clave: Confidencialidad, Integridad y Disponibilidad (Tríada CIA).
- Amenazas frecuentes: Phishing, Malware, Ransomware, Ingeniería social.
- Modelo de capas de defensa: múltiples barreras para reducir riesgos.
- Ejemplo práctico: Analizar un correo sospechoso y detectar señales de phishing.
- Ejercicio: Identificar elementos inseguros en un ejemplo real de correo.

Buenas Prácticas y Capas de Defensa

- Contraseñas únicas y seguras (mínimo 12 caracteres, combinación de letras, números y símbolos).
- Mantener actualizaciones automáticas activas en sistemas y aplicaciones.
- No abrir adjuntos ni enlaces desconocidos.
- Uso de antivirus, firewall y sentido común como capas de defensa.
- Ejercicio: Dibujar un esquema de tus capas de seguridad personal.

Módulo 2 · Cuentas y Dispositivos seguros

- Uso de gestores de contraseñas (Bitwarden, 1Password, Google Password Manager).
- Creación de passphrases: Ejemplo → 'MiCasaAzul2025EsSegura!'
- Autenticación en dos pasos (MFA/2FA): aplicaciones autenticadoras vs. SMS.
- Ejemplo práctico: Activar MFA en Gmail o redes sociales.
- Ejercicio: Crear una passphrase y verificar su fortaleza en passwordmeter.net.

Higiene de Dispositivos

- Activar actualizaciones automáticas del sistema operativo y antivirus.
- Bloquear el equipo al ausentarse (Windows + L / Ctrl + Cmd + Q).
- Cifrado del disco y respaldo periódico de la información.
- Navegadores seguros: configuración de privacidad y bloqueo de rastreadores.
- Ejercicio técnico: Activar cifrado BitLocker o FileVault según tu sistema operativo.

Módulo 3 · Redes y protección de datos

- Buenas prácticas en Wi-Fi doméstico: cambiar contraseña del router y ocultar SSID.
- Redes públicas: evitar ingresar contraseñas o datos personales.
- Uso de VPN: cuándo sí (trabajo remoto, Wi-Fi público) y cuándo no (servicios bancarios).
- Estrategia 3-2-1 de copias de seguridad: 3 copias, 2 medios distintos, 1 en la nube.
- Ejercicio: Configurar un respaldo automático semanal de tus archivos.

Módulo 4 · Respuesta ante Incidentes

- Señales de compromiso: lentitud del sistema, ventanas emergentes, correos extraños.
- Qué hacer ante un incidente: desconectar, informar y no borrar evidencias.
- Herramientas útiles: VirusTotal, HavelBeenPwned, Windows Defender Logs.
- Ejercicio: Verificar una URL o archivo sospechoso en virustotal.com.
- Caso práctico: Simular respuesta a un ataque de phishing.

Conclusión

- La ciberseguridad no depende solo de la tecnología, sino del comportamiento consciente de cada persona.
- Durante este curso aprendiste a identificar amenazas comunes, proteger tus cuentas y dispositivos, fortalecer tus contraseñas, y actuar ante incidentes de seguridad.
- La clave está en aplicar lo aprendido de forma constante: actualizar tus equipos, verificar enlaces antes de hacer clic, usar autenticación en dos pasos y respaldar tu información regularmente.
- Recuerda: **la mejor defensa es la prevención**.
  Cada buena práctica que adoptes protege no solo tus datos, sino también los de tu familia, tu trabajo y tu entorno digital.
- 🔒 *"La seguridad digital comienza contigo."*