La Salle
Instituto San Carlos
Medellín

TALLER DE PLAN DE MEJORAMIENTO PERIODO I

Periodo	I	Grupo	10°	Area	Tecnología e Informática.
Alumno (a)					
Maestro	Andrés Carmona Velásquez				
Indicadores de Desempeño	Saber: Comprende el impacto en la sociedad y reconoce la importancia de las normas de seguridad y los derechos de autor. Hacer: Aplica normas de seguridad, utiliza licencias y derechos de autor de manera adecuada, y propone soluciones tecnológicas para abordar problemas específicos. Ser: Demuestra un compromiso ético y responsable hacia el uso de la tecnología e informática, reconociendo su influencia en la sociedad y la cultura.				

Actividades	Fecha
Desarrolla el siguiente taller en hojas de bloc, escritas a mano con letra legible. Lee cuidadosamente cada caso antes de responder. SECCIÓN I: Selección Múltiple (Única Respuesta) *Escribe en tu hoja el número de la pregunta y la letra de la respuesta correcta, justificando brevemente por qué la elegiste.* 1. (Seguridad de Contraseñas) Un usuario crea la contraseña M1P3rrOTOb1! para su correo. Aunque tiene mayúsculas, números y símbolos, el usuario sube fotos diarias de su perro Tobi a sus redes sociales públicas. ¿Por qué esta contraseña representa un riesgo de seguridad? A. Porque los sistemas actuales no reconocen el símbolo "!" en las bases de datos. B. Porque es vulnerable a la ingeniería social, ya que un atacante puede deducirla observando su huella digital pública. C. Porque es demasiado corta y un ataque de fuerza bruta la descifraría en un segundo. D. Porque los números están intercalados con las letras de manera incorrecta. 2. (Big Brother) En el contexto tecnológico actual, el concepto del "Gran Hermano" (Big Brother) ya no se refiere a un dictador vigilando por cámaras de televisión, sino a: A. Los virus informáticos que dañan el hardware de los computadores. B. El sistema de algoritmos y recolección masiva de datos (compras, ubicación, likes) que perfila y predice el comportamiento de los ciudadanos. C. Los hackers éticos que intentan proteger a los usuarios de las estafas. D. El monopolio de las empresas de telecomunicaciones sobre la velocidad del internet. 3. (Phishing) Recibes un mensaje de texto que dice: *"Tu cuenta bancaria ha sido bloqueada por seguridad. Para evitar la cancelación total, haz clic aquí y actualiza tus datos en los próximos 15 minutos: http://banco-seguridad-alerta.com"*. ¿Cuál es la táctica psicológica principal que usa este mensaje para engañarte?	Entrega del trabajo 19 de marzo 2026

A. Ofrecer un premio o beneficio económico inesperado.
B. Generar un sentido de urgencia extrema y miedo a perder algo importante para que actúes sin pensar.
C. Apelar a la confianza utilizando el nombre de un familiar cercano.
D. Utilizar lenguaje técnico complejo para confundir al usuario.

4. (Permisos de Aplicaciones) Descargas una aplicación gratuita de linterna para tu celular. Al abrirla, te pide permiso para acceder a tu ubicación GPS y a tu micrófono. ¿Cuál es la lectura crítica que debes hacer de esta situación?

A. La aplicación necesita el micrófono para encender la luz mediante comandos de voz.
B. Es un procedimiento estándar de seguridad de las tiendas de aplicaciones para evitar virus.
C. Si el producto es gratis, el modelo de negocio probablemente sea recolectar mis datos (audio y ubicación) para venderlos a anunciantes.
D. Los permisos son obligatorios y no afectan en nada la privacidad del dispositivo.

5. (Integración de Riesgos) ¿Cómo se relacionan los permisos innecesarios en el celular con el concepto de la "Huella Digital"?

A. No se relacionan, ya que la huella digital solo se forma por lo que publicamos voluntariamente en redes sociales.
B. Los permisos concedidos alimentan nuestra huella digital pasiva, entregando datos invisibles sobre nuestra rutina diaria sin que nos demos cuenta.
C. Revocar permisos borra automáticamente toda nuestra huella digital del pasado.
D. Las aplicaciones con muchos permisos protegen nuestra identidad en internet.

SECCIÓN II: Análisis y Pensamiento Crítico (Preguntas Abiertas)

Responde las siguientes preguntas en tu hoja de trabajo con argumentos claros, evitando respuestas de "sí o no".

1. Sobre el Phishing: En ciberseguridad se dice que *"el eslabón más débil de un sistema informático no es la máquina, sino el ser humano"*. Explica con tus propias palabras qué significa esta frase usando como ejemplo un ataque de Phishing.
2. Sobre los Permisos del Celular: Imagina que auditas el celular de un amigo y descubres que una aplicación de "Juegos de Carreras" tiene acceso a su cámara frontal y a sus contactos. Explícale a tu amigo, en al menos tres líneas, cuáles son los riesgos reales de privacidad a los que se está exponiendo.
3. Sobre el Big Brother: Muchas personas justifican entregar todos sus datos diciendo: *"No me importa que me vigilen, no tengo nada malo que ocultar"*. ¿Qué argumento le darías a esa persona para demostrarle que la vigilancia extrema (como el crédito social o el perfilamiento por algoritmos) sí puede afectarle de forma negativa, incluso si es un "buen ciudadano"?

SECCIÓN III: Escrito Crítico (Síntesis) Instrucción: Escribe un texto argumentativo de **exactamente dos párrafos** bien estructurados donde conectes los cuatro temas vistos. • **Párrafo 1:** Explica cómo el descuido en los **permisos de las aplicaciones** en nuestro celular alimenta el sistema de vigilancia del **"Big Brother"** moderno. • **Párrafo 2:** Concluye explicando cómo toda esa información que regalamos facilita que seamos víctimas de ataques de **Phishing** hiperpersonalizados y por qué una **contraseña** fuerte no sirve de nada si caemos en la ingeniería social.	

Firma Docente	Firma Alumno