Universidad Nacional de Ingeniería (UNI)
Escuela Profesional de
Ciberseguridad
Sílabo 2024-II

1. CURSO

CY261. Seguridad Humana (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CY261. Seguridad Humana
2.2 Semestre	:	8^{vo} Semestre.
2.3 Créditos	:	3
2.4 horas	:	2 HT; 2 HP;
2.5 Duración del periodo	:	16 semanas
2.6 Condición	:	Obligatorio
2.7 Modalidad de aprendizaje	:	Presencial
2.8 Prerrequisitos	:	CS3I1. Seguridad en Computación. (7^{mo} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso explora la dimensión humana de la ciberseguridad, analizando el comportamiento humano en relación con la seguridad de la información y los sistemas. Se abordan temas como ingeniería social, gestión de identidad, conciencia de riesgos, privacidad y factores humanos en el diseño de sistemas seguros, capacitando a los estudiantes para comprender y mitigar los riesgos asociados al factor humano.

5. OBJETIVOS

- Comprender la influencia del comportamiento humano en la ciberseguridad.
- Analizar las vulnerabilidades y amenazas relacionadas con el factor humano.
- Aplicar estrategias para promover una cultura de seguridad y fortalecer la seguridad humana en las organizaciones.

6. RESULTADOS DEL ESTUDIANTE

3) Comunicarse efectivamente en diversos contextos profesionales. (Usage)

4) Reconocer las responsabilidades profesionales y tomar decisiones informadas en la práctica de la computación basadas en principios legales y éticos. (Assessment)

6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas. (Usage)

7. TEMAS

Unidad 1: Gestión de identidad (10 horas)	
Resultados esperados: 3,4,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Identificación y autenticación de personas y dispositivos. – Este tema proporciona una descripción general de varios métodos de control de acceso para demostrar los beneficios y desafíos de cada uno. – Los temas incluyen una descripción general del control de acceso a la red (NAC) – Gestión de acceso a identidades (IAM) – roles – multimétodo – sistemas de identificación y autenticación – sistemas de autenticación biométrica (incluidas cuestiones como precisión/FAR/FRR, resistencia, privacidad, etc.) – usabilidad y tolerabilidad de los métodos. • Control de activos físicos y lógicos. – cubre varios controles de acceso a activos físicos, incluido hardware del sistema, activos de red, dispositivos de respaldo/almacenamiento, etc. Algunos ejemplos son el control de acceso a la red (NAC), la gestión de acceso a identidades (IAM), el control de acceso basado en reglas (RAC), el control de acceso basado en roles (RBAC), métodos de seguimiento de inventario y métodos de creación de identidad (qué tipo de ID de usuario ayuda a aumentar la seguridad con el control de acceso, por ejemplo, abc1234, nombre y apellido, inicial del primer nombre y apellido). • Identidad como servicio (IaaS) – Este tema cubre la gestión de identidades como servicio (por ejemplo, identidad en la nube) y plantea problemas como que el sistema está fuera del control del usuario sin forma de saber qué ha sucedido con la información en el sistema, auditar el acceso, garantizar el cumplimiento y la flexibilidad para revocar permisos rápidamente. • Servicios de identidad de terceros – Este tema proporciona una descripción general de la infraestructura de autenticación utilizada para crear, alojar y administrar servicios de identidad de terceros. – Los temas incluyen local, nube, servicios de identidad centralizados/herramientas de administración de contraseñas, administración de privilegios de punto final, etc. • Ataques de control de acceso y medidas de mitigación – Este tema proporciona una descripción general	• Explique la diferencia entre identificación, autenticación y autorización de acceso de personas y dispositivos [Usar] • Analice la importancia de los registros de auditoría y de la identificación y autenticación del inicio de sesión [Usar] • Demostrar la capacidad de implementar el concepto de privilegio mínimo y segregación de funciones [Usar] • Demostrar la comprensión general de los ataques de control de acceso y las medidas de mitigación [Usar]

Unidad 2: Ingeniería social (12 horas)

Resultados esperados: 3,4,6

Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Tipos de ataques de ingeniería social – Este tema proporciona una descripción general de las diferentes formas en que los ciberdelincuentes o grupos maliciosos explotan las debilidades en las organizaciones, los sistemas, las redes y la información personal utilizada para permitir un ciberataque posterior. – Los temas propuestos incluyeron: ataques de phishing y phishing, suplantación física/suplantación de identidad, vishing (phishing telefónico), vulneración del correo electrónico y cebo. • Psicología de los ataques de ingeniería social – Este tema proporciona una descripción general de los factores psicológicos y de comportamiento relacionados con las personas que caen en ataques de ingeniería social. – Los temas propuestos incluyen el pensamiento contradictorio, cómo las respuestas emocionales impactan la toma de decisiones, sesgos cognitivos de riesgos y recompensas, y creación de confianza. • Usuarios engañosos – Este tema proporciona una descripción general de las interfaces de los sistemas de mensajes y de los navegadores y/o la interacción del usuario que pueden explotarse para engañar a los usuarios. – Los temas propuestos incluyen suplantación de remitentes de mensajes, URL engañosas, cómo los usuarios juzgan y confían en las páginas web y los correos electrónicos, así como el comportamiento de los usuarios con phishing y otras advertencias del navegador. • Detección y mitigación de ataques de ingeniería social – Este tema proporciona actividades prácticas basadas en escenarios mediante simulación o herramientas virtuales para crear un entorno de diversos ataques de ingeniería social. – Experiencia práctica en el uso de herramientas y enfoques técnicos para detectar y/o mitigar diferentes amenazas de ingeniería social. – Herramientas propuestas como filtrado de correo electrónico, listas negras, herramientas de gestión de eventos e información de seguridad (SIEM) e IDS/IPS.	• Demostrar comprensión general de los tipos de ataques de ingeniería social, la psicología de los ataques de ingeniería social y engañar a los usuarios [Usar] • Demostrar la capacidad de identificar tipos de ataques de ingeniería social [Usar] • Demostrar la capacidad de implementar enfoques para la detección y mitigación de ataques de ingeniería social [Usar]

Lecturas : [**Mitnick2002**]

Unidad 3: Cumplimiento personal de las reglas/políticas/normas éticas de ciberseguridad (8 horas)	
Resultados esperados: 4,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Mal uso del sistema y mala conducta del usuario – Este tema proporciona una descripción general del mal uso intencional y no intencional del sistema, el ciberacoso, el ciberpirateo, el comportamiento ingenuo y los dilemas éticos relacionados con las decisiones de seguridad del sistema. • Cumplimiento y reglas de comportamiento. – Este tema proporciona una descripción general de los métodos y técnicas para lograr que las personas sigan las reglas/políticas/normas éticas (por ejemplo, ¡conducir!). • Comportamiento adecuado bajo incertidumbre – Este tema proporciona una descripción general de los métodos y técnicas a seguir cuando no se está seguro de cómo responder a una situación de ciberseguridad. – . Los temas incluyen CyberIQ, adaptabilidad intelectual, pensamiento crítico, comprensión de las decisiones correctas versus incorrectas, cómo tomar esas decisiones en condiciones de incertidumbre, pensamiento racional versus irracional, pensamiento/decisiones éticas y comportamiento cuando no hay un proceso claro a seguir (informes/punto de contacto/etc.) y mitigación de errores humanos.	• Demostrar comprensión general de los tipos de ataques de ingeniería social, la psicología de los ataques de ingeniería social y engañar a los usuarios [Usar] • Demostrar la capacidad de identificar tipos de ataques de ingeniería social [Usar] • Demostrar la capacidad de implementar enfoques para la detección y mitigación de ataques de ingeniería social [Usar] • Discutir la importancia de la ciberhigiene, la educación de los usuarios en ciberseguridad, así como la concientización sobre las cibervulnerabilidades y amenazas [Usar] • Describir los temas principales dentro de los programas de Educación, Capacitación y Concientización sobre Seguridad (SETA) [Usar] • Discuta la importancia de SETA como contramedidas [Usar] • Discutir la importancia de la percepción y comunicación del riesgo en el contexto de los modelos mentales de ciberseguridad y privacidad [Usar]
Lecturas : [**Olson2008**]	

Unidad 4: Conciencia y comprensión (10 horas)	
Resultados esperados: 3,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Percepción y comunicación del riesgo – Este tema cubre cómo los usuarios perciben y responden a los riesgos de ciberseguridad, los sesgos cognitivos al juzgar los riesgos, las metáforas para comunicar riesgos de seguridad particulares y cómo formular mensajes sobre los riesgos. – Definición de modelo mental, cómo los modelos mentales impactan el comportamiento del usuario, así como modelos mentales comunes (modelos populares) de ciberseguridad y privacidad. • Higiene cibernética – Este tema proporciona una discusión y actividades centradas en las responsabilidades individuales (no de la organización) para proteger y mitigar contra las ciberamenazas y los ciberataques. – Los temas incluyen creación de contraseñas, almacenamiento de contraseñas, herramientas de mitigación (es decir, software antivirus), cómo identificar sitios web seguros, identificar niveles de configuración de privacidad, etc.). • Educación de usuarios en ciberseguridad – Métodos para educar a los usuarios finales sobre diversas amenazas y comportamientos en materia de ciberseguridad/privacidad – Los temas incluyen métodos para crear conciencia entre los usuarios (PreK-12, empleados, público, etc.), métodos de impartición de educación y capacitación en ciberseguridad (por ejemplo, carteles, folletos, capacitación por computadora, gamificación, estilos de comunicación, formulación de mensajes, cómo llegar diferentes audiencias y comunidades de usuarios, personas con discapacidades y/o deterioros cognitivos), el momento oportuno y el refuerzo de la educación, así como el impacto de la formación en los conocimientos y comportamientos de los usuarios. • Concientización sobre vulnerabilidades y amenazas cibernéticas – Este tema proporciona una descripción general de las amenazas que enfrenta el usuario final, así como del miedo, la incertidumbre y la duda (FUD). Los temas propuestos incluyen señales de advertencia de vulnerabilidades y amenazas internas de los empleados, conciencia sobre el robo de identidad, compromiso del correo electrónico empresarial, amenaza de redes Wi-Fi abiertas/libres y malware, spyware y ransomware.	• Discutir la importancia de la ciberhigiene, la educación de los usuarios en ciberseguridad, así como la concientización sobre las cibervulnerabilidades y amenazas [Usar] • Describir los temas principales dentro de los programas de Educación, Capacitación y Concientización sobre Seguridad (SETA) [Usar] • Discuta la importancia de SETA como contramedidas [Usar] • Discutir la importancia de la percepción y comunicación del riesgo en el contexto de los modelos mentales de ciberseguridad y privacidad [Usar]

Unidad 5: Privacidad social y conductual (8 horas)	
Resultados esperados: 3,4	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Teorías sociales de la privacidad – Este tema proporciona una descripción general de varias teorías de la privacidad de la psicología social y las ciencias sociales, enfatizando la privacidad que implica interactuar con otras personas en lugar de organizaciones. Los temas propuestos incluyen compensaciones y riesgos de privacidad en el contexto social, control y conciencia del consentimiento de datos, monitoreo de información personal, protecciones regulatorias y preocupaciones sobre el mantenimiento de la privacidad social. • Privacidad y seguridad de las redes sociales – Decisiones y comportamientos de divulgación en línea de los usuarios – Personas y gestión de identidad – Determinación de controles de audiencia y acceso social – Interfaz y mecanismos de afrontamiento para gestionar la privacidad en varios sitios de redes sociales. – Desafíos de gestionar los límites del tiempo. – Así como los límites personales/laborales de las redes sociales.	• Comparar y contrastar diversas teorías de la privacidad de la psicología social y las ciencias sociales [Usar] • Describir los conceptos de compensaciones y riesgos de privacidad en el contexto social, control y conocimiento del consentimiento de datos, monitoreo de información personal, protecciones regulatorias y preocupaciones sobre el mantenimiento de la privacidad social [Usar] • Discuta la importancia de la privacidad y seguridad de las redes sociales [Usar]
Lecturas : [**Acquisti2015**]	

8. PLAN DE TRABAJO

8.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

8.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

8.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

9. SISTEMA DE EVALUACIÓN

********* EVALUATION MISSING ********

10. BIBLIOGRAFÍA BÁSICA