Sílabo de Seguridad de la Información Corporativa

I. Datos generales

Código	ASUC 00769			
Carácter	Electivo			
Créditos	3			
Periodo académico	2020			
Prerrequisito	Ninguno			
Horas	**Teóricas:**	2	**Prácticas:**	2

II. Sumilla de la asignatura

La asignatura corresponde al área de estudios de especialidad electiva, es de naturaleza teórico-práctica. Tiene como propósito desarrollar en el estudiante la capacidad de usar diferentes modelos de seguridad asociados al manejo de confidencialidad, integridad y disponibilidad, en el marco global de los diferentes estándares de seguridad en TI.

La asignatura contiene: Introducción a la seguridad de la información. Sistemas de control de acceso y su metodología. Arquitecturas de seguridad y sus modelos. Seguridad en las operaciones. Criptografía. Sistema de autenticación y cifrado. Seguridad perimetral. Seguridad por contenidos. Seguridad en el ciclo de vida de las aplicaciones. Seguridad de entornos físicos. CyberSeguridad, y Tecnologías de Seguridad.

III. Resultado de aprendizaje de la asignatura

Al finalizar la asignatura, el estudiante será capaz de proteger la información de las organizaciones de los diferentes riesgos informáticos que puedan alterar o dañar los recursos informáticos, por medio de diversos mecanismos de seguridad siguiendo las técnicas de seguridad y las mejores prácticas de la industria relacionadas con seguridad de la información.

IV. Organización de aprendizajes

<table>
<tr><td colspan="3">Unidad I
Principios de seguridad de la información y control de accesos</td><td>Duración en horas</td><td>16</td></tr>
<tr><td>Resultado de aprendizaje de la unidad</td><td colspan="4">Al finalizar la unidad, el estudiante será capaz de proteger los activos de información de una organización a nivel de acceso lógico y a nivel de personas.</td></tr>
<tr><td colspan="2">Conocimientos</td><td>Habilidades</td><td colspan="2">Actitudes</td></tr>
<tr><td colspan="2">✓ Pilares de la seguridad de la información
✓ Control de accesos
✓ Ingeniería social</td><td>✓ Identifica los diversos riesgos inherentes al uso de la tecnología.
✓ Identifica las fases, técnicas y escenarios relacionados al control de accesos y los mecanismos de identificación, de autenticación y de autorización.
✓ Identifica los diversos escenarios en que los atacantes realizan la ingeniería social y determina defensas efectivas contra este tipo de ataques.</td><td colspan="2">✓ Asume el compromiso de revisar los contenidos previos al dictado de la clase.</td></tr>
<tr><td>Instrumento de evaluación</td><td colspan="4">• Rúbrica de evaluación
• Lista de cotejo</td></tr>
<tr><td>Bibliografía (básica y complementaria)</td><td colspan="4">Básica:
• International organization for standardization. (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. ISO/IEC.
• Isaca. (2014). CISM Review Manual. (13° ed.). EEUU: ISACA.

Complementaria:
• Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK, Fourth Edition. USA: (ISC)2 Press.
• Harris, S. (2013). CISSP All-In-One Exam Guide, (6° ed.) USA: McGraw-Hill.
• Greenwald G. (2014). Snowden: sin un lugar para esconderse. Barcelona: Ediciones B.
• Mitnick, K., Wozniak S. (2012). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. USA: Little, Brown and Company.</td></tr>
<tr><td>Recursos educativos digitales</td><td colspan="4">• Curso contexto e introducción a la seguridad: https://www.coursera.org/learn/information-security-data</td></tr>
</table>

<table>
<tr><td colspan="2">Unidad II
Controles de seguridad</td><td>Duración en horas</td><td>16</td></tr>
<tr><td>Resultado de aprendizaje de la unidad</td><td colspan="3">Al finalizar la unidad, el estudiante será capaz de implementar controles de seguridad relacionados al malware, controles criptográficos, controles a la infraestructura y controles a las redes para evitar los riesgos relacionados.</td></tr>
<tr><td>Conocimientos</td><td>Habilidades</td><td colspan="2">Actitudes</td></tr>
<tr><td>✓ Seguridad contra el malware
✓ Criptografía
✓ Seguridad de infraestructura
✓ Seguridad de redes</td><td>✓ Prepara los mecanismos de defensa contra las diferentes amenazas e identifica las relacionadas al malware: virus, gusanos, troyanos, rootkits, botnets, ransomware entre otros.
✓ Aplica la criptografía simétrica, asimétrica y las funciones hash e identifica los diversos escenarios donde se aplica la criptografía
✓ Identifica los controles de protección a Nivel de Data Center, a nivel de los endpoints, que incluye: Servidores, laptops, móviles.
✓ Identifica los controles a Nivel de Redes LAN, WAN, WLAN.</td><td colspan="2">✓ Participa activamente en el desarrollo de las actividades grupales en clase.</td></tr>
<tr><td>Instrumento de evaluación</td><td colspan="3">• Rúbrica de evaluación
• Lista de cotejo</td></tr>
<tr><td>Bibliografía (básica y complementaria)</td><td colspan="3">Básica:
• International organization for standardization. (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. ISO/IEC.
• Isaca. (2014). CISM Review Manual. (13° ed.). EEUU: ISACA.

Complementaria:
• Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK, Fourth Edition. USA: (ISC)2 Press.
• Harris, S. (2013). CISSP All-In-One Exam Guide, (6° ed.) USA: McGraw-Hill.
• Greenwald G. (2014). Snowden: sin un lugar para esconderse. Barcelona: Ediciones B.
• Mitnick, K., Wozniak S. (2012). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. USA: Little, Brown and Company.</td></tr>
<tr><td>Recursos educativos digitales</td><td colspan="3">• Curso de Malware
https://www.coursera.org/learn/malsoftware</td></tr>
</table>

<table>
<tr><td colspan="2">Unidad III
Seguridad del Internet, Cloud Computing y dispositivos móviles</td><td>Duración en horas</td><td>16</td></tr>
<tr><td>Resultado de aprendizaje de la unidad</td><td colspan="3">Al finalizar la unidad, el estudiante será capaz de aplicar controles de seguridad para proteger los datos que fluyen hacia y desde el Internet, así como proteger las iniciativas de Cloud Computing y la información residente en los dispositivos móviles inteligentes que los usuarios utilizan de manera ubicua.</td></tr>
<tr><td>Conocimientos</td><td>Habilidades</td><td colspan="2">Actitudes</td></tr>
<tr><td>✓ Seguridad de Internet
✓ Ciberseguridad y cibercrimen
✓ Seguridad del Cloud Computing
✓ Seguridad de los dispositivos móviles</td><td>✓ Identifica las amenazas provenientes del Internet y los principales actores: crackers, script-kiddies, lammers, wannabies; analizando las razones y acciones del Hackactivismo.
✓ Identifica los riesgos del cibercrimen y el ciberespionaje, el impacto de los ataques de ciber-seguridad en las Organizaciones y las estrategias para combatir el cibercrimen.
✓ Aplica los controles a implementar para minimizar los riesgos al uso del Cloud Computing, identificando las amenazas provenientes del Cloud Computing y determina los diversos modelos del Cloud Computing
✓ Aplica los controles a implementar para minimizar los riesgos de la movilidad de la información; analizando el fenómeno de consumerización de la tecnología, identificando los riesgos del uso de los diversos dispositivos móviles y los diferentes riesgos por Sistema Operativo Movil: Android vs. iOS.</td><td colspan="2">✓ Participa activamente en clases a través de preguntas, comentarios y ejemplos.</td></tr>
<tr><td>Instrumento de evaluación</td><td colspan="3">• Rúbrica de evaluación
• Lista de cotejo</td></tr>
<tr><td>Bibliografía (básica y complementaria)</td><td colspan="3">Básica:
• International organization for standardization. (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. ISO/IEC.
• Isaca. (2014). CISM Review Manual. (13° ed.). EEUU: ISACA.

Complementaria:
• Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK, Fourth Edition. USA: (ISC)2 Press.
• Harris, S. (2013). CISSP All-In-One Exam Guide, (6° ed.) USA: McGraw-Hill.
• Greenwald G. (2014). Snowden: sin un lugar para esconderse. Barcelona: Ediciones B.
• Mitnick, K., Wozniak S. (2012). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. USA: Little, Brown and Company.</td></tr>
<tr><td>Recursos educativos digitales</td><td colspan="3">• Curso de Ciberseguridad https://www.coursera.org/specializations/cybersecurity-developing-program-for-business
• Curso Seguridad de moviles
• https://www.academiaeset.com/default/store/14041-seguridad-en-dispositivos-moviles</td></tr>
</table>

<table>
<tr><td colspan="3">Unidad IV
Seguridad de sistemas de información, bases de datos y tecnologías de seguridad</td><td>Duración en horas</td><td>16</td></tr>
<tr><td>Resultado de aprendizaje de la unidad</td><td colspan="4">Al finalizar la unidad, el estudiante será capaz de aplicar controles de seguridad en los sistemas de información, aplicaciones y bases de datos y adquirir tecnología de seguridad en función al riesgo y a las necesidades de protección de información de las organizaciones.</td></tr>
<tr><td colspan="2">Conocimientos</td><td>Habilidades</td><td colspan="2">Actitudes</td></tr>
<tr><td colspan="2">✓ Controles de seguridad en los Sistemas de Información
✓ Controles de seguridad en las Bases de Datos
✓ Tecnologías de Seguridad de protección de datos
✓ Tecnologías de Seguridad de Sistemas de Información
✓ Tecnologías de Seguridad de protección de infraestructura tecnológica
✓ Tecnologías de Seguridad de protección de usuarios</td><td>✓ Aplica controles de seguridad en los sistemas de información, aplicaciones y bases de datos
✓ Identifica controles de seguridad para desarrollar software seguro, para implementar bases de datos seguras.
✓ Selecciona las diversas tecnologías y productos existentes en el mercado de manera adecuada para proteger los datos, los sistemas de información, la infraestructura y a los usuarios.</td><td colspan="2">✓ Muestra actitudes innovadoras ganar – ganar, persistencia positiva, entusiasmo y trabajo en equipo.</td></tr>
<tr><td>Instrumento de evaluación</td><td colspan="4">• Rúbrica de evaluación
• Lista de cotejo</td></tr>
<tr><td>Bibliografía (básica y complementaria)</td><td colspan="4">Básica:
• International organization for standardization. (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. ISO/IEC.
• Isaca. (2014). CISM Review Manual. (13° ed.). EEUU: ISACA.

Complementaria:
• Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK, Fourth Edition. USA: (ISC)2 Press.
• Harris, S. (2013). CISSP All-In-One Exam Guide, (6° ed.) USA: McGraw-Hill.
• Greenwald G. (2014). Snowden: sin un lugar para esconderse. Barcelona: Ediciones B.
• Mitnick, K., Wozniak S. (2012). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. USA: Little, Brown and Company.</td></tr>
<tr><td>Recursos educativos digitales</td><td colspan="4">• Curso Seguridad del Software
https://www.coursera.org/learn/software-security</td></tr>
</table>

V. Metodología

El desarrollo de la asignatura será mediante investigación previa de los estudiantes de los conocimientos requeridos, seguido de una exposición teórica complementaria con apoyo audiovisual, y una activa participación de los estudiantes, con tratamiento y exposición de casos en clase, revisión y debate de los controles de lectura asignados y planteamiento de problemas y participación general en la solución de los mismos.

Se publicarán casos de discusión semanales, planteamiento de situaciones de auditoría real y participación general en la definición del informe de riesgos de auditoría.

Se distribuirá material digital de lectura y casos previos a cada clase, haciendo uso de mecanismos virtuales. El material deberá ser estudiado y desarrollado por el estudiante.

VI. Evaluación

VI.1. Modalidad presencial

Rubros	Comprende	Instrumentos	Peso
Evaluación de entrada	Prerrequisitos o conocimientos de la asignatura	Prueba objetiva	Requisito
Consolidado 1	Unidad I	Rubrica de evaluación	20%
	Unidad II	Lista de cotejo	
Evaluación parcial	Unidad I y II	Prueba de desarrollo	20%
Consolidado 2	Unidad III	Rubrica de evaluación	20%
	Unidad IV	Lista de cotejo	
Evaluación final	Todas las unidades	Rubrica de evaluación	40%
Evaluación sustitutoria (*)	Todas las unidades	No aplica	

(*) Reemplaza la nota más baja obtenida en los rubros anteriores

VI.2. Modalidad semipresencial

Rubros	Comprende	Instrumentos	Peso
Evaluación de entrada	Prerrequisito	Prueba objetiva	Requisito
Consolidado 1	Unidad I	Rubrica de evaluación	20%
Evaluación parcial	Unidad I y II	Prueba de desarrollo	20%
Consolidado 2	Unidad III	Rubrica de evaluación	20%
Evaluación final	Todas las unidades	Rubrica de evaluación	40%
Evaluación sustitutoria (*)	Todas las unidades	No aplica	

(*) Reemplaza la nota más baja obtenida en los rubros anteriores

Fórmula para obtener el promedio:

PF = C1 (20%) + EP (20%) + C2 (20%) + EF (40%)

Mg. Felipe Néstor Gutarra Meza
Decano
Universidad Continental

Firmado por
FELIPE NÉSTOR GUTARRA MEZA
CN = FELIPE NÉSTOR GUTARRA MEZA
O = UNIVERSIDAD CONTINENTAL
T = DECANO
Date: 17/08/2020 04:23