|  |  |  |
| --- | --- | --- |
|  | **FUNDACIÓN UNIVERSITARIA UNINPAHU** | |
| **VICERRECTORIA ACADÉMICA** | |
| **FORMATO DE ESPACIO ACADÉMICO** | |
| **FACULTAD: INGENIERIA Y TECNOLOGIA DE LA INFORMACION** | |
| **PROGRAMA: INGENIERÍA DE SOFTWARE** | |
| **TIPO DE FORMACIÓN: PROFESIONAL** | |
| **NOMBRE DEL ESPACIO ACADÉMICO: SEGURIDAD INFORMÁTICA**  xxxxxxx | |
| **Carácter del espacio académico: TEÓRICO: TEÓRICO-PRÁCTICO: PRÁCTICO:**  v | |
| **Código: IS1699** | **Código: IS1699** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Número Total de Créditos**  **Académicos:** | **Número Total de Horas**  **Semanales:** | | **Número Total de Horas**  **Semanales de**  **Trabajo Directo:** | **Número Total de Horas Semanales de**  **Trabajo**  **Independiente:** | **Modalidad** | |
| Presencial | X |
| 3 | 3 | | 3 | 6 | Distancia |  |
| Virtual |  |
| **Componente al que pertenece:** | |  | | | | |

|  |
| --- |
| **JUSTIFICACIÓN** |
| La utilización de medios computacionales para almacenar, transferir y procesar información se ha convertido en elemento indispensable para el funcionamiento de la sociedad. Como consecuencia, la información es un activo valioso que se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad.  Las nuevas oportunidades de negocio vienen fundamentadas en el uso de nuevas tecnologías, la economía digital, utiliza herramientas tecnológicas como estrategias novedosas con el propósito de propender a la competitividad en el marco de la globalización económica. Por eso el incremento de aplicaciones electrónicas como correo, comercio, transacciones y dinero electrónicos, firmas y certificados digitales, acceso seguro a bancos de información y comunicaciones seguras, entre otras; En Colombia, la existencia de recursos humanos especializados en Seguridad Informática es escasa y el uso de tecnologías nacientes implica riesgos significativos en el manejo de la información, el amplio desarrollo de la tecnologías informáticas abre espacio a conductas antisociales con la posibilidad de cometer delitos tradicionales en formas no tradicionales. Por esto es necesario implementar modelos de seguridad de la información que prevengan y reaccionen ante la posible pérdida o afectación de la información del negocio. |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INTENCIONALIDAD PEDAGÓGICA** | | | | | | | | | |
| **Objetivos de aprendizaje** | | | | | **Objetivos de enseñanza** | | | | |
| El estudiante comprenderá los conceptos fundamentales y los principios básicos de la Seguridad Informática, las formas de atentados, los delitos informáticos, la capa 2 del modelo OSI, los puertos y servicios, reduciendo el riesgos de seguridad al mínimo, reconociendo metodologías que le permitirán implantar un sistema de gestión de riesgos en la organización y así mismo, Identificándolas políticas, controles, los estándares y normas necesarios para un SGSI en una organización. | | | | | Formar Profesionales que conozcan las normatividad y estándares nacionales e Internacionales en las áreas de Seguridad Informática para así dar respuesta a los requerimientos de las organizaciones tanto públicas, privadas y comunidad en General.  Plantear un Modelo Seguro de la Tecnología de la información tomando en cuenta las normas y estándares aplicables, los fundamentos de SI, con la implementación de los controles adecuados al escenario de aplicación y elaborando políticas de seguridad. | | | | |
| **METODOLOGÍA** | | | | | | | | | |
| Presentación de quizes, los parciales y exámenes finales, elaboración de Resúmenes y tareas ya que esta técnica permite repasar rápidamente un tema en la cual representa de forma abreviada y precisa el contenido de un documento, sin interpretación crítica y sin distinción del autor del análisis, para lo cual se deberá subrayar las partes principales del texto, tomar nota de las ideas más significativas y apuntar palabras clave. Mapas conceptuales y Mapas Mentales Corresponde a esquemas conceptuales de la lectura de temas de los contenidos del curso o lecturas propuestas, los cuales serán realizadas como actividad individual habrán espacios interacción directa con el docente estarán dados por los debates generados con respecto a temas del curso, consultas propuestas Juicio de valor individual sobre el trabajo realizado y las competencias alcanzadas.  Será presencial, correspondiente a los temas del contenido programático y consultas propuestas donde se realizaran talleres, investigaciones, proyectos, etc.  Y para la digitación de notas se tendrá en cuenta el porcentaje de cada uno de los cortes así:  Primer corte: 30%  Segundo corte: 30%  Tercer corte: 40% | | | | | | | | | |
| **UNIDADES Y TEMATICAS** | | | | | | | | | |
| **Unidad** | **Tema** | | | | | **Semanas** | | **Tipo de contenido (actitudinales, conceptuales o procedimentales)** | |
| 1 | •Historia de la Seguridad  • Concepto e Importancia de la Seguridad Informática  • Principios básicos de la Seguridad Informática: Confidencialidad, Integridad y Disponibilidad  • Principios Fundamentales de la Seguridad Informática  • Autenticación, Control de Acceso, No Repudio y Observancia  •Entidades y organismos asociados a la Seguridad Informática. (ORGANIZACIONES)  • Certificaciones profesionales  • Oportunidades laborales y de desarrollo profesional  •Normatividad en Colombia Ley 1293 de 2009  •Ley 527 De 1999  • Ley 1581 de 2009  • Conpes 3701 "Lineamientos de política para la Ciberseguridad y Ciberdefensa" para Colombia  •Concepto básicos sobre hackers y crakers | | | | | Semana 1-5 | | Conceptuales y/o procedimentales | |
| 2 | •Mitos de la seguridad en capa 2  •Por qué? asegurar la capa 2  •Segmentación y Fragmentación  •Fragmentación Patológica  • Esteganografía y Criptografía  •Definición de Amenazas, Vulnerabilidades y Riesgos  •Conceptos sobre riesgos y sistemas de administración de riesgos  • Los 6 elementos del Riesgo  • Metodología para implantar un sistema de gestión de riesgos  • Estándares internacionales y nacionales de administración de riesgos  • Ejemplos de sistema de gestión de riesgos  • Medición de Riesgos | | | | | Semana 5-11 | | Conceptuales y/o procedimentales | |
| 3 | •Conceptos de SGSI.  • Políticas de Seguridad  • Controles de Seguridad  • Métricas de Seguridad  • Generalidades de un SGSI  • La ISO 27001 e ISO 27002  • Documentación requerida para un SGSI  • Roles y responsabilidades de un SGSI  • Herramientas que apoyan un SGSI  • Auditoria ISO 27001 | | | | | Semana 11-16 | | Conceptuales y/o procedimentales | |
| **EVALUACIÓN DEL APRENDIZAJE** | | | | | | | | | |
| Competencia Global (Tobón (2004)) | | Saberes esenciales | Unidades de Competencia / Rango de aplicación | | | | | | |
| Insuficiente  (0-29) | Aceptable  (30-39) | | | Sobresaliente  (40-45) | | Excelente  (46-50) |
| Desarrollar proyectos de TI, Servicios de TI y planes de trabajo para satisfacer los requerimientos de las organizaciones de acuerdo a las necesidades de transformación de estas usando herramientas, modelos, tecnologías y estándares vigentes. | | Ejecuta con responsabilidad las tareas asignadas de acuerdo a talleres presentando cumplidamente y de acuerdo a las rubricas del trabajo autónomo y de clase | Entrega actividades incompletas fuera del intervalo de fechas  Falta continuamente a clase sin excusa o llega tarde continuamente | No siempre Entrega a tiempo las actividades  Algunas actividades están completas y otras no  Suele fallar a clase o llegar tarde  Evidencia trabajo fuera del aula | | | Entrega a tiempo las actividades  La mayoría de actividades evidencian completitud  Algunas veces no es cumplido en el horario de clase  Evidencia trabajo fuera del aula de clase  En el aula se comporta adecuadamente | | Entrega a tiempo las actividades evidenciando completitud  Evidencia trabajo fuera del aula de clase  En el aula se comporta adecuadamente y es cumplido en el horario de clase |
| Reconoce los riesgos de vulnerabilidad en los sistemas informáticos. | No describe modelos de administración de riesgos. | Describe algunos modelos de administración de riesgos. | | | Describe la mayoría de modelos de administración de riesgos. | | Describe los modelos de administración de riesgos. |
| Establece seguimiento a procesos de seguridad informática  Elabora modelos de seguridad para sistemas de información. | No esquematiza las técnicas de auditoría. | Esquematiza pocas técnicas de auditoría. | | | Esquematiza algunas de las técnicas de auditoría. | | Esquematiza las técnicas de auditoría. |
| No Aplica metodologías a vectores de ataque | Aplica pocas metodologías a vectores de ataque | | | Aplica algunas metodologías a vectores de ataque | | Aplica metodologías a vectores de ataque |
| **PREGUNTAS ORIENTADORAS** | | | | | | | | | |
| A medida que las corporaciones, los particulares y nuestra economía dependen cada vez más de Internet y de los sistemas informáticos, los riesgos de dichos sistemas se hacen mucho más evidentes e incrementan su importancia, lo cual abarca muchas preguntas como:   1. Que es la Tecnología, y como hacer uso de ella? 2. ¿Es siempre positivo utilizar la tecnología? ¿hay alguna razón para no hacerlo? 3. ¿La tecnología evoluciona rápidamente,  qué habrá dentro de 10 años. ¿Podemos saberlo? 4. ¿Cuáles son los dispositivos electrónicos más utilizados? 5. Las redes sociales, ¿son un terreno peligroso como nos muestran muchas veces los medios de comunicación? ¿o un lugar lleno de oportunidades y diversión? ¿por qué existen estas dos visiones tan diferentes sobre las redes sociales? 6. ¿Cuáles son las amenazas en Internet? ¿y cuáles son las medidas principales para estar protegidos? 7. Los riesgos informáticos pueden estar relacionados con la pérdida potencial de información y la recuperación de dichos datos o con el uso permanente de la información? 8. Los problemas o los fallos de los sistemas informáticos ocasionan graves crisis empresariales y/o daños en la reputación? | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
| **RELACIÓN CON LA INVESTIGACIÓN Y LA PROYECCCIÓN SOCIAL DEL PROGRAMA** | | | | | | | | | |
| **Relación del espacio académico con la investigación en el programa:** El espacio académico es práctico ya que cuenta con máquinas y programas para diferentes talleres y ejercicios donde el estudiante aprenderá los conceptos y técnicas básicas de la informática por medio de programas y herramientas modernas incentivando al estudiante a la investigación y proyección social del programa. | | | | | | | | | |
| **BIBLIOGRAFÍA, HEMEROGRAFÍA Y WEBGRAFÍA COMPLEMENTARIA** | | | | | | | | | |
| Bibliografía básica:   * SIYAN, K y HARE, C. (1995) Internet y Seguridad en Redes. Prentice Hall. * ANONIMO. (2000) Linux Máxima Seguridad. Prentice Hall. * SIYAN, K. (2001) Microsoft Windows 2000 TCP/IP. Prentice Hall. * GONCALVES, M; et al. (1997) Internet Privacy Kit. Que. * NORTHCUTT, S y NOVAK, J. (2001) Detección de Intrusos. Prentice Hall. * MC CLURE, S y SCAMBRAY, J. (2002) HACKERS en Windows 2000. Mc Grad Hill. * SCAMBRAY, J y SCHEMA, M. (2003) HACKERS de Sitios Web. McGraw Hill. * HATCH, B y LEE, J. (2003) HACKERS en Linux 2a Ed. McGraw Hill. * KURTZ, G; HATCH, B y LEE, J. (2001) HACKERS en Linux. McGraw Hill. * MC CLURE, S; SCAMBRAY, J y KURTZ, G. (2002) | | | | | | | | | |
| Bibliografía complementaria:   * HACKERS 3. McGraw Hill. O ´DEA, M. (2004) CLAVES HACKERS en Windows. McGraw Hill. * DHANJANI, N. (2004) CLAVES HACKERS en Linux y Unix. McGraw Hill. * SHEMA, M. (2004) CLAVES HACKERS de Sitios Web. McGraw Hill. * SCHIFFMAN, M; O´DONELL, A y POLINO, D. (2003) HACKERS, 19 Desafíos Prácticos más. Mc Graw Hill. * RIOS, R. (2003) La Conspiración HACKER. Longseller. * HIMANEN, P. (2003) La Ética del Hacker. Ediciones Destino. * VERTON, D. (2004) BLACK ICE, La Amenaza Invisible del Ciberterrorismo. Mc Graw Hill. * TORRIJOS, VICENTE. "Hacia la seguridad convergente: Escenarios de transformación y cambio en la defensa y la seguridad hemisférica y global". Editorial Universidad del Rosario (2013). * KYRIAZOGLOU, JOHN. "CONTROLES DE LA SEGURIDAD DE LA TI". IT Governance Publishing (2013) * Pinilla F, José Dagoberto. LAS NORMAS DE AUDITORÍA INFORMÁTICA. Colombia 2010. | | | | | | | | | |
| Cybergrafía:  <http://www.iso27001standard.com/es/que-es-iso-27001/>  <http://www.jstor.org/action/doBasicSearch?Query=seguridad+informatica&prq=cobit+5.0&group=none&fc=off&acc=off&hp=25&wc=on&so=rel>  <http://descargadicto.net/ebooks/269718/redusers-seguridad-informaticapdf-mega.html>  <https://www.isotools.org/2015/09/22/4-documentos-en-pdf-para-aprender-sobre-seguridad-informatica/>  <http://www.apser.es/blog/2015/11/02/consejos-utiles-de-seguridad-informatica-en-pdf/> | | | | | | | | | |
| Audiovisuales | | | | | | | | | |
| Enlaces de Internet | | | | | | | | | |