|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PROGRAMA UNIDAD CURRICULAR** | | | | | | | | | |
| Unidad Académica | | | DEPARTAMENTO DE ECONOMÍA, PRODUCCIÓN E INNOVACIÓN TECNOLÓGICA | | | | | | |
| Carrera/s | | | LICENCIATURA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN | | | | | | |
| Plan de Estudios | | | Resolución (CS) 220/2019 | | | | | | |
| 1. Datos sobre la unidad curricular | | | | | | | | | |
| Nombre | Seguridad Informática | | | | | | Código | 6031 | |
| Modalidad | Presencial | | | Régimen | | Cuatrimestral. | | | |
|
| Equipo responsable | | | Lic. Sergio Eduardo Torres. | | | | | | |
| Año y mes de presentación del programa | | | 2023-Marzo | | | | | | |
| 1. Carga horaria | | | | | | | | | |
| Horas de clase semanales | | 4 | | |  | | | |  |
| Horas de clase totales | | 64 | | | Horas totales teóricas | | | |  |
| Horas totales prácticas | | | |  |
| Otras horas totales (laboratorio, trabajo de campo, etc.) | | | |  |

|  |  |
| --- | --- |
| 1. Unidades correlativas precedentes en el Plan de Estudios | |
| Denominación | Código |
| Laboratorio de Programación y Lenguajes | 6017 |
| Programación Orientada a Objetos | 6018 |
| Comunicaciones y Redes | 6022 |
| Ingeniería de Software II | 6023 |

|  |
| --- |
| 1. Contenidos mínimos según Plan de Estudios |
| Fundamentos de seguridad informática. Factores humanos, lógico y físico. Políticas, y procedimientos de seguridad. Área de seguridad informática en una organización. Vulnerabilidades de sistemas informáticos. Arquitecturas de seguridad en sistemas informáticos de organizaciones. Planes de contingencias y continuidad de negocios. Leyes, normas, regulaciones sobre delitos informáticos. Auditoría, peritaje e informática forense. |

|  |
| --- |
| 1. Fundamentación |
| Seguridad Informática es una unidad curricular que proveerá a sus estudiantes el conocimiento necesario para modelar, implementar, operar, monitorear, revisar, mantener y mejorar continuamente esquemas de gestión de la seguridad de la información.  La continuidad de los procesos de las organizaciones tiene como uno de sus pilares sostener la infraestructura tecnológica que refiere a la captura, procesamiento y obtención de información en sus operaciones. El perfil de Licenciado en Gestión de la Tecnología de la Información debe aprender a comprender los aspectos técnicos y su dinámica en el contexto actual, de forma de poder identificar y gestionar esquemas de seguridad informática.  En ese sentido, se abordan los contenidos esenciales relacionados con la protección de la información vista como uno de los principales activos de las organizaciones, basándose en un aprendizaje de experiencias en diferentes organizaciones, un aprendizaje cooperativo y un aprendizaje autónomo. |

|  |
| --- |
| 1. Objetivos |
| El objetivo general de la unidad curricular es que los estudiantes logren la capacidad de demostrar conocimiento en el campo de la gestión en seguridad de la información, comprendiendo y aplicando los conceptos principales de la seguridad informática y los factores intervinientes en el marco de las problemáticas de las organizaciones, según las leyes, normas y regulaciones vigentes.  Conocimientos para adquirir:   * Un conocimiento profundo de los conceptos principales de seguridad de la información y de las tecnologías de ciberseguridad y/o ciberdefensa. * Un conocimiento esencial sobre la teoría y la aplicación de la seguridad de la información en redes informáticas y en el desarrollo del software. * Un conocimiento profundo sobre la gestión de aspectos vinculados a la seguridad de la información en organizaciones tanto públicas como privadas.   Habilidades para desarrollar:   * Integrar conocimientos de las materias correlativas para la comprensión del problema de la seguridad de la información, relacionando los aspectos técnicos informáticos con los aspectos de gestión de las organizaciones. * Aprender a planificar y realizar una investigación guiada limitada basada en la bibliografía de esta unidad curricular. * Comprender la criticidad sobre disponer y evaluar información actualizada relativa a la seguridad de la información y aprender los mecanismos necesarios para su obtención. * Desarrollar una actitud crítica y reflexiva respecto a la temática de la seguridad informática, mediante la concientización de las posibles consecuencias que aborde esta materia. * Planificar e investigar las últimas tendencias en el área de Seguridad Informática, relacionada a los contenidos que abarca esta unidad curricular.   Competencias:   * Comprender los objetivos de la seguridad de la información en relación con los activos de una organización, identificando las potenciales amenazas y escenarios de vulnerabilidad. * Realizar análisis sobre el estado de situación respecto la seguridad informática en una   organización.   * Entender los requerimientos de seguridad de la información de una organización, necesidades de políticas y procedimientos. * Gestionar procesos de implementación y operación de controles respecto de la seguridad de la información. * Comprender globalmente los aspectos de la seguridad de la información en la industria y los mercados, tanto a nivel técnico como de negocios. |

|  |
| --- |
| 1. Contenidos (organizados por unidades) |
| UNIDAD 1: Seguridad informática.  Seguridad de la información. Terminología. Disponibilidad. Confiabilidad. Integridad. Riesgos, amenazas, vulnerabilidades y ataques. Factores humanos, lógico y físico. Medidas de protección. Plan de continuidad del negocio. Marco de trabajo de seguridad informática.  UNIDAD 2: Seguridad física.  Componentes de la seguridad física. Tipos de amenazas a la seguridad física. Seguridad de centros de procesamiento de la información. Controles de acceso. Esquemas de copias de respaldo y recuperación de información.  UNIDAD 3: Seguridad en redes de información.  Seguridad de la red. Capa de seguridad de transporte. Seguridad perimetral. Detección y prevención de intrusos. Seguridad en redes inalámbricas. Redes privadas virtuales. Criptografía. Funciones de hash. Infraestructura de clave pública. Firma digital. Estenografía.  UNIDAD 4: Seguridad en el desarrollo de software.  Mecanismos de seguridad en sistemas operativos. Seguridad de aplicaciones. Control de acceso. Esquemas de implementación de autenticación y autorización. Seguridad en aplicaciones web, tipos de vulnerabilidades y medidas de protección.  Gestión de la seguridad. Políticas. Procedimientos. Áreas de seguridad informática. Equipos de respuesta. Centros de operaciones de seguridad. Estándares. Normas, leyes, regulaciones. Educación en seguridad informática. Perfiles profesionales de seguridad informática. Ética y seguridad informática. Delitos informáticos. Ley de propiedad intelectual. Ley de Delitos Informáticos. Auditoría. Peritaje. Forensia informática. |

|  |
| --- |
| 1. Bibliografía obligatoria y complementaria (organizada por unidades) |
| UNIDAD 1: Seguridad informática  Bibliografía obligatoria:   * ISO 22301: (2012). Societal security, Business continuity management systems, Requirements.Caro, R., & Sánchez, E. (2017). Ciberseguridad y Protección de la Información. Ra-ma Editorial. * Sanz, A. (2018). Seguridad Informática: Conceptos y herramientas. Paraninfo. * Gómez, M. J. (2017). Auditoría Informática y Seguridad en Sistemas de Información. Ediciones Paraninfo. * González, J. C. (2017). Protección de datos personales: fundamentos, normativa y práctica. Editorial Reus. * Llopis, J. (2019). El gran libro de la seguridad informática. Grupo Anaya Comercial. * García, A. (2019). Ciberseguridad y Ciberdefensa: Introducción a la Seguridad Informática. Ediciones Paraninfo. * Pérez, R. M. (2019). Análisis Forense Informático: Técnicas, Herramientas y Prácticas para la Investigación de Delitos Informáticos. Ediciones Paraninfo. * Stallings, W. (2016). Cryptography and Network Security: Principles and Practice.   Seventh Edition. Global Edition. Pearson. Capítulo 1.   * Stallings, W., Brown, L. (2018). Computer security: principles and practice, Fourth Edition, Global edition. Pearson. Capítulos 1, 6. * Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework). Capítulos 1 y 2. * Shirey, R. (2007). RFC 4949: Internet security glossary 2. * ISO/IEC 27031 (2011). Information technology, Security techniques, Guidelines for information and communication technology readiness for business continuity.   Bibliografía complementaria:   * ISO/IEC 27000 (2018). Information technology, Security techniques, Information security management systems, overview and vocabulary. * Harris, S., & Maymi, F. (2018). CISSP All-in-One Exam Guide, book. McGraw Hill Education. * Vieites, Á. G. (2011). Enciclopedia de la seguridad informática Grupo Editorial RA-MA. * Huamán Rivera, O. R. (2018). Diseño de un sistema de gestión de continuidad operativa para una entidad pública bajo el enfoque de la norma ISO/IEC 22301: 2012. * Wong, W. N. Z., & Shi, J. (2014). Business Continuity Management System: A Complete Guide to Implementing ISO 22301. Kogan Page Publishers.   UNIDAD 2: Seguridad física  Bibliografia obligatoria:   * Tanenbaum, A. S., & Bos, H. (2015). Sistemas Operativos Modernos. Pearson Educación. * García, A. (2019). Fundamentos de Redes de Computadoras: Conceptos, Principios y Tecnologías. Ediciones Paraninfo. * Hernández, J. A., & Alarcón, E. (2017). Sistemas Distribuidos: Conceptos y Diseño. Ediciones Paraninfo. * Bravo, M. G. (2019). Arquitectura de Computadoras: Un Enfoque Cuantitativo. Pearson Educación. * Vargas, A. (2019). Big Data: Conceptos, Herramientas y Tecnologías. Ediciones Paraninfo. * Cortés, A. C. (2017). Seguridad en Redes y Comunicaciones. Ediciones Paraninfo. * García, A. (2017). Seguridad Informática: Métodos y Técnicas para la Protección de Sistemas de Información. Ediciones Paraninfo. * Stallings, W., Brown, L. (2018). Computer security: principles and practice. Fourth Edition. Global Edition. Pearson. Capítulos 5, 16. * Silberschatz, A., Gagne, G., & Galvin, P. B. (2018). Operating system concepts. Tenth Edition. Wiley. Capítulos 11, 14.   Bibliografia Complementaria:   * Telecommunication Industry Association. (2017). TIA-942-B data center standards overview.   UNIDAD 3: Seguridad en redes de información  Bibliografia obligatoria:   * Forouzan, B. A. (2015). Comunicación de Datos y Redes de Computadoras. McGraw-Hill. * Kurose, J. F., & Ross, K. W. (2016). Redes de Computadoras: Un Enfoque Descendente Basado en Internet. Pearson Educación. * Behrouz, A. F. (2015). Protocolos de Interconexión de Redes. McGraw-Hill. * Cisco Networking Academy. (2019). CCNA 1: Introducción a las redes. Cisco Press. * Odom, W. (2019). Guía de Certificación de CCENT/CCNA ICND1 100-105. Pearson Educación. * González, M. J. (2017). Análisis y Diseño de Redes: Metodología y Herramientas Prácticas. Marcombo. * Laquey, T. (2015). Internet: Un Mundo de Oportunidades Para Todos. Addison Wesley. * Stallings, W. (2014). Data and Computer Communications. Tenth Edition. Pearson. Capítulos 13, 14, 23. * Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Seventh Edition. Global Edition. Pearson. Capítulos 3, 9, 10, 11, 13, 14, 17, 18.   Bibliografia Complementaria   * Stallings, W., Brown, L. (2018). Computer security: principles and practice. Fourth Edition. Global Edition. Pearson. Capítulos 2, 8, 9, 21, 22, 23 y 24. * Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Seventh Edition. Global Edition. Pearson. Capítulo 16.   UNIDAD 4: Seguridad en el desarrollo de software  Bibliografía obligatoria:   * García, R. (2018). Seguridad Informática: Preparación para la certificación CompTIA Security+. Díaz de Santos. * Pacheco, R. (2017). Seguridad en Sistemas Informáticos. Anaya. * Riesgo, J. M. (2016). Hacking ético: Cómo proteger empresas y personas frente al hacking. Anaya. * Goodrich, M. T., Tamassia, R., & Goldwasser, M. H. (2013). Introducción a la Seguridad Informática. Pearson Educación. * Alvarez, J. C. (2018). Análisis Forense Digital. Marcombo. * Castro, R., & Gasti, K. (2018). Introducción a la criptografía. Universidad de La Rioja. * González, J. (2016). Guía de Seguridad de la Información. Fondo Editorial USMP. * Stallings, W., Brown, L. (2018). Computer security: principles and practice. Fourth   Edition. Global Edition. Pearson. Capítulos 3, 4, 5, 11, 12.   * Silberschatz, A., Gagne, G., & Galvin, P. B. (2018). Operating system concepts. Tenth Edition. Wiley. Capítulos 9, 16 y 17. * STOCK, A. V. D., et al. (2017). OWASP Top 10 2017. The Ten Most Critical Web Application Security Risks.   Bibliografía complementaria:   * Messier, R. (2015). Operating system forensics. Elsevier, Syngress. * Messier, R. (2019). CEH v10 Certified Ethical Hacker Study Guide. Sybex. |

|  |
| --- |
| 1. Metodología de trabajo |
| El desarrollo de las clases estará de acuerdo con criterios que garantizarán el aprovechamiento del tiempo destinado al proceso de formación, focalizando el tiempo de clase en la comprensión conceptual y desarrollo de las capacidades de aprendizaje de la temática de seguridad, guiando al desarrollo de habilidades prácticas, y fomentando la lectura domiciliaria.  El dictado de las clases se realizará de manera tal que el proceso de enseñanza y aprendizaje permita una efectiva transferencia de conocimientos y comunicación de experiencias relevantes.  En las clases se presentarán los temas en exposiciones orales, se harán referencias al material bibliográfico, se realizarán experimentos prácticos y se estudiarán casos reales de aplicación.  En cada clase y cuando lo amerite la correlación de temas, se hará un repaso sintético de los  contenidos de la clase anterior y además habrá un espacio con la finalidad de evacuar posibles dudas que los estudiantes posean.  Respecto al cronograma de dictado de clases, la primera clase se realizará la presentación de la unidad curricular y los temas a tratar, y se hará un repaso general del contenido que se toma de las unidades curriculares correlativas. Además, se dictará una clase de repaso de todos los temas tratados en el día de clase previo a examen.  Se complementará el dictado de clases con material disponible en el campus virtual de la UNPaz. |

|  |
| --- |
| 1. Evaluación |
| Evaluaciones parciales  Se proveerán dos instancias de evaluaciones parciales:  Evaluación Parcial I - EXAMEN PARCIAL INDIVIDUAL:   * Evaluación Teórica y práctica. Individual. Presencial, en horario de cursada. De producción escrita. * Opcionalmente, la parte teórica se podrá rendir por adelantado y por partes mediante   cuestionarios individuales de producción escrita durante el transcurso y en el comienzo del horario de la cursada. La parte teórica representa el 50% de la nota del examen parcial individual. El 50% restante correspondiente a la parte práctica que no se podrá rendir por partes.  Evaluación Parcial II - TRABAJO TEÓRICO-PRÁCTICO GRUPAL:   * Evaluación teórica y práctica. Grupal. Domiciliaria (de producción escrita, con posibilidad de entregas parciales) y presencial (de producción oral).   Ambas evaluaciones tendrán una nota correspondiente al esquema de calificación. Estas dos notas serán tenidas en cuenta como base para la aprobación de la Unidad Curricular.   * Evaluación Teórica y práctica. Individual. Presencial, en horario de cursada. De producción escrita.   Criterios de Evaluación:   * Conocimientos teóricos: se evaluará la comprensión y asimilación de los conceptos y fundamentos teóricos de la seguridad informática, así como la capacidad de aplicarlos en la resolución de problemas. * Habilidades prácticas: se evaluará la capacidad de los estudiantes para aplicar las técnicas y herramientas de seguridad informática en la práctica, y para resolver problemas relacionados con la seguridad en sistemas informáticos. * Trabajo en equipo: se evaluará la capacidad de los estudiantes para trabajar en equipo y colaborar con otros en la realización de proyectos y tareas relacionadas con la seguridad informática. * Comunicación y presentación: se evaluará la capacidad de los estudiantes para comunicar sus ideas y conocimientos de manera clara y efectiva, tanto de forma oral como escrita, en informes, presentaciones y trabajos prácticos. * Ética: se evaluará el compromiso de los estudiantes con la ética y la responsabilidad en la práctica de la seguridad informática, incluyendo la protección de la privacidad y los derechos de los usuarios y la aplicación de los principios de confidencialidad, integridad y disponibilidad de la información. * Participación y asistencia: se evaluará la participación y el compromiso de los estudiantes con la materia, su capacidad para cumplir con las tareas y proyectos asignados y su asistencia a clases y actividades de la materia.   Recuperatorios:  Existirá una instancia de recuperación para cada evaluación parcial. A la misma podrán acceder aquellos/as estudiantes que:   * Hayan obtenido una calificación inferior a 7 (siete) puntos. * Hayan estado ausente de forma debidamente justificada.   Todas las instancias de recuperación serán individuales, de producción oral y escrita en el caso de la Evaluación Parcial I y de producción escrita en el caso de la evaluación parcial II.  La calificación que los/as estudiantes obtengan en la instancia de recuperatorio reemplazará la calificación obtenida en el examen que se ha recuperado y será la considerada definitiva a los efectos de la aprobación.  Escala de calificación  Todas las calificaciones serán en escala numérica y conceptual, del 1 (uno) al 10 (diez). Los estudiantes podrán solicitar, una vez realizada la calificación, se les dé vista y/o una fundamentación explícita del resultado obtenido.  Requisitos de aprobación  Se establecen los siguientes mecanismos de aprobación:   * Mediante promoción directa: quienes hayan obtenido una calificación de 7 (siete) o más puntos como promedio de todas las instancias evaluativas, sean estas parciales o sus recuperatorios, debiendo obtener una nota igual o mayor a 6 (seis) puntos en cada una de estas. * Mediante aprobación de examen integrador: quienes hayan obtenido una calificación entre 4 (cuatro) y 6 (seis) puntos en promedio de las instancias parciales y como mínimo un 4 (cuatro) en cada instancia o en sus respectivos recuperatorios. El examen será de modalidad escrita. * Mediante examen final: hayan obtenido una calificación entre 4 (cuatro) y 6 (seis) en los respectivos exámenes parciales y/o sus recuperatorios, pero no hubieren aprobado o asistido a la instancia del examen integrador. * Mediante examen libre: en aplicación del Régimen de Aprobación en Exámenes Libres. |

|  |
| --- |
| 1. Instancias de práctica (si corresponde) |
| --------------------------------------------------------------------------------------------------------------- |

|  |  |
| --- | --- |
| 1. Cronograma de actividades | |
| Semana 1 | Presentación de la materia. UNIDAD 1: Seguridad informática |
| Semana 2 | UNIDAD 1: Seguridad informática |
| Semana 3 | UNIDAD 2: Seguridad física |
| Semana 4 | UNIDAD 2: Seguridad física |
| Semana 5 | UNIDAD 3: Seguridad en redes de información |
| Semana 6 | UNIDAD 3: Seguridad en redes de información |
| Semana 7 | UNIDAD 3: Seguridad en redes de información  UNIDAD 3: Seguridad en redes de información |
| Semana 8 | UNIDAD 3: Seguridad en redes de información |
| Semana 9 | Evaluación Parcial I. |
| Semana 10 | UNIDAD 4: Seguridad en el desarrollo de software  Instancia de recuperación de la Evaluación Parcial I. |
| Semana 11 | UNIDAD 4: Seguridad en el desarrollo de software |
| Semana 12 | UNIDAD 4: Seguridad en el desarrollo de software |
| Semana 13 | UNIDAD 4: Seguridad en el desarrollo de software |
| Semana 14 | UNIDAD 4: Seguridad en el desarrollo de software |
| Semana 15 | Evaluación Parcial II. |
| Semana 16 | Instancia de recuperación de la Evaluación Parcial II. Clase de Cierre. |

|  |  |
| --- | --- |
| *A partir de aquí completar únicamente las unidades curriculares con régimen anual* | |
| Semana 17 | ------------------------------------------------------------------------------------------- |
| Semana 18 | ------------------------------------------------------------------------------------------- |
| Semana 19 | ------------------------------------------------------------------------------------------- |
| Semana 20 | ------------------------------------------------------------------------------------------- |
| Semana 21 | ------------------------------------------------------------------------------------------- |
| Semana 22 | ------------------------------------------------------------------------------------------- |
| Semana 23 | ------------------------------------------------------------------------------------------- |
| Semana 24 | ------------------------------------------------------------------------------------------- |
| Semana 25 | ------------------------------------------------------------------------------------------- |
| Semana 26 | ------------------------------------------------------------------------------------------- |
| Semana 27 | ------------------------------------------------------------------------------------------- |
| Semana 28 | ------------------------------------------------------------------------------------------- |
| Semana 29 | ------------------------------------------------------------------------------------------- |
| Semana 30 | ------------------------------------------------------------------------------------------- |
| Semana 31 | ------------------------------------------------------------------------------------------- |
| Semana 32 | ------------------------------------------------------------------------------------------- |

Firma del docente/s responsable/s:

~~Texto, Carta

Descripción generada automáticamente~~