****

 UNIVERSIDAD NACIONAL

 “JOSÉ FAUSTINO SÁNCHEZ CARRIÓN”

 **VICERRECTORADO ACADÉMICO**

**FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS**

1

**E INFORMÁTICA**

**ESCUELA PROFESIONAL DE INGENIERÍA**

**DE SISTEMAS**

**MODALIDAD NO PRESENCIAL**

**SÍLABO POR COMPETENCIAS**

**CURSO:**

**SEGURIDAD INFORMÁTICA**

1. **DATOS GENERALES**

|  |  |
| --- | --- |
| Línea de carrera | Tecnologías de Información y Comunicación |
| Semestre académico | 2020 - I |
| Código del curso | 3205501 |
| Créditos | 3 |
| Horas Semanales | Hras. Totales: 4 Teóricas: 2 Prácticas: 2 |
| Ciclo | IX |
| Sección | A |
| Apellidos y Nombres del Docentes | Barrera Loza, Ana Doris Magdalena |
| Correo Institucional | abarrera@unjfsc.edu.pe  |
| N de Celular | 945217272 |

1. **SUMILLA**

La asignatura Seguridad Informática se encuentra dentro de los cursos de especialidad, en la línea de Seguridad Informática. Es de tipo teórico práctico, debido al avance de la tecnología y la ciencia, la gestión de la información y el conocimiento, por lo que el propósito del curso es que los alumnos gestionen la seguridad de la información en cualquier tipo de empresa. Cuenta con 4 unidades didácticas cuyo contenido es el siguiente: Seguridad informática. Objetivos. Áreas. Causas de la inseguridad. Activos. Amenazas. Vulnerabilidad. Riesgo e impacto en los negocios. Gestión de la Seguridad de la Información. Serie Norma ISO 27000. ISO 27001. Control de Accesos. Mecanismos de Seguridad. Ataques informáticos. Seguridad en Base de Datos. Seguridad en las redes. Informática forense. Políticas de seguridad.

**DESCRIPCIÓN DEL CURSO.**

Con la proliferación de la tecnología han aparecido notables riesgos que pueden atentar contra el funcionamiento de los sistemas, sometidos a ataques por una creciente comunidad de delincuentes informáticos. La existencia de estos riesgos y mecanismos para su detección, mitigación o recuperación obligan al profesional informático incorporar a su perfil las competencias que posibiliten evaluar e implementar medidas de seguridad en sus sistemas.

Para un estudiante de **Ingeniería de Sistemas** es necesario y fundamental tener un conocimiento solido sobre la gestión de la seguridad de la información con el fin de desarrollar su capacidad de lógica y racionamiento para solucionar problemas relacionados con la identificación y tratamiento de los riesgos para contribuir en tomas de decisiones en forma eficiente y eficaz dentro de una organización, de tal forma que la puedan aplicar en su desarrollo profesional, una vez que egresen de la Universidad.

En el proceso de la formación del Ingeniero de Sistemas debe incorporarse como diseñar el plan de seguridad que debería adoptar una empresa para prevenir, impedir, reducir controlar los riesgos que soporta un sistema de información y el entorno asociado con él; entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.

3

1. **CAPACIDADES AL FINALIZAR EL CURSO**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **CAPACIDAD DE LA UNIDAD DIDACTICA** | **NOMBRE DE LA****UNIDAD DIDACTICA** | **SEMANAS** |
| **UNIDAD I** | Administra los elementos de la gestión de la seguridad de la información dentro de una empresa para asegurar la integridad de la información según ciclo de Deming | INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN | 1-4 |
| **UNIDAD II** | Gestiona los controles de accesos necesarios en una empresa para el aseguramiento de su información de acuerdo a un sistema de avance tecnológico. | CONTROL DE ACCESOS | 5-8 |
| **UNIDAD III** | Propone los mecanismos de seguridad que se pueden implementar en una empresa de acuerdo a su realidad para evitar ataques de intrusos siguiendo recomendaciones internacionales  | MECANISMOS DE SEGURIDAD | 9-12 |
| **UNIDAD IV** | Evalúa los diferentes tipos de ataques que pueden sufrir sus sistemas de redes y bases de datos, para implementar políticas de seguridad de las mismas de acuerdo a las recomendaciones de normas. | SEGURIDAD EN REDES Y BASES DE DATOS | 13-16 |

1. **INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO**

|  |  |
| --- | --- |
| **N** | **INDICADORES DE CAPACIDAD AL FINALIZAR EL CURSO** |
| 1 | Identifica los elementos y la importancia de la seguridad informática. |
| 2 | Identifica correctamente los diferentes activos de información en una empresa. |
| 3 |  Desarrolla un sistema de Gestión de la Seguridad de la Información en una empresa.  |
| 4 | Aplica la gestión de riesgos que se debe tener en una organización. |
| 5 | Aplica las recomendaciones de la Serie Norma ISO 27000. ISO 27001. |
| 6 | Aplica los controles de acceso dentro de una organización. |
| 7 | Aplica los diferentes mecanismos de identificación. |
| 8 | Implementa los diferentes mecanismos de autentificación. |
| 9 | Aplica las principales reglas y políticas para la creación y administración de contraseñas. |
| 10 | Implementa los diferentes sistemas biométricos, dentro de una organización. |
| 11 | Aplica los diferentes controles criptográficos dentro de las organizaciones. |
| 12 | Reconoce los diferentes métodos de ataques informáticos.  |
| 13 | Implementa adecuadamente controles de seguridad en las bases de datos. |
| 14 | Implementa adecuadamente controles de seguridad en las redes. |
| 15 | Aplica adecuadamente la informática forense. |
| 16 | Diseña e implementa políticas de seguridad dentro de una organización. |

**V. DESARROLLO DE LAS UNIDADES DIDACTICAS:**

|  |  |
| --- | --- |
| **UNIDAD DIDACTICA I :**  **INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN** | **CAPACIDAD DE LA UNIDAD DIDACTICA I:** Administra los elementos de la gestión de la seguridad de la información dentro de una empresa para asegurar la integridad de la información según ciclo de Deming |
| **SEMANA** | **CONTENIDOS** | **ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL** | **INDICADORES DELOGRO DE LA CAPACIDAD** |
| **CONCEPTUAL** | **PROCEDIMENTAL** | **ACTITUDINAL** |
| ***1*** | Introducción a la seguridad Informática. Principios. Seguridad informática. Objetivos. Áreas. | Analiza los elementos de seguridad de la información y su importancia dentro de las organizaciones. | Trabajo en equipo para discutir los conceptos de seguridad de la información. | **Clase expositiva** (Docente/Alumno)* Uso del Google Meet

**Debate dirigido** (Discusiones)* Foros, chat

**Lecturas*** Uso de repositorios digitales

**Lluvia de ideas (Saberes previos)*** Foros, chat
 | Identifica los elementos y la importancia de la seguridad de la información. |
| ***2*** | Activos. Amenazas. Vulnerabilidad. Riesgo e impacto en los negocios. Inventario de Activos.  | Analiza y comprende la importancia de los activos de información y sus vulnerabilidades. | Trabajo en equipo para realizar el inventario de activos de una organización. | Identifica correctamente los diferentes activos de información en una empresa. |
| ***3*** | Gestión de la Seguridad de la Información. Beneficios. Ciclo de Deming. Planificar y Hacer. Alcance.  | Analiza y comprende el sistema de Gestión de la Seguridad de la Información y sus ventajas. | Acrecienta el interés sobre el sistema de Gestión de la Seguridad de la Información. | Desarrolla un sistema de Gestión de la Seguridad de la Información en una empresa. |
| ***4*** | Gestión de riesgos. Análisis de riesgos. Tratamiento de riesgos. Declaración de aplicabilidad. Implementación del SGSI. Revisar y actuar.  | Comprenderla Gestión de riesgos. Análisis de riesgos. Tratamiento de riesgos.  | Trabajo en equipo para acrecentar el interés sobre cómo gestionar los riesgos, su Análisis y Tratamiento de riesgos.  | Aplica la gestión de riesgos que se debe tener en una organización. |
|  | **EVALUACIÓNDE LA UNIDAD DIDÁCTICA** |
| **EVIDENCIA DE CONOCIMIENTO** | **EVIDENCIA DE PRODUCTO** | **EVIDENCIA DE DESEMPEÑO** |
| * Argumentación de la importancia de la seguridad de la información.
 | * Exposiciones sobre la implementación de un SGSI.
 | * Comportamiento en clase virtual y chat.
 |

|  |  |
| --- | --- |
| **UNIDAD DIDACTICA II : CONTROL DE ACCESOS** | **CAPACIDAD DE LA UNIDAD DIDACTICA II:** Gestiona los controles de accesos necesarios en una empresa para el aseguramiento de su información de acuerdo a un sistema de avance tecnológico. |
| **SEMANA** | **CONTENIDOS** | **ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL** | **INDICADORES DELOGRO DE LA CAPACIDAD** |
| **CONCEPTUAL** | **PROCEDIMENTAL** | **ACTITUDINAL** |
| ***5*** | Serie Norma ISO 27000. ISO 27001. Beneficios. Implementación. Certificación. | Comprende la Serie Norma ISO 27000, ISO 27001 y sus beneficios. | Trabajo en equipo para discutir cómo implementar las recomendaciones de la Serie Norma ISO 27000. ISO 27001.  | **Clase expositiva** (Docente/Alumno)* Uso del Google Meet

**Debate dirigido** (Discusiones)* Foros, chat

**Lecturas*** Uso de repositorios digitales

**Lluvia de ideas (Saberes previos)*** Foros, chat
 | Aplica las recomendaciones de la Serie Norma ISO 27000. ISO 27001. |
| ***6*** | Control de Accesos. Principios. Categorías de control de Acceso.  | Analiza y determina que tipos de control de acceso se debe implementar según el tipo de información. | Propicia el trabajo en equipo para analizar y determina que tipos de control de acceso se debe implementar en una organización. | Aplica los controles de acceso dentro de una organización. |
| ***7*** | Técnicas de control de accesos. Identificación, Autenticación, Autorización.  | Diferencia entre lo que es identificación, autenticación y autorización. | Acrecienta el interés sobre los mecanismos de identificación. | Aplica los diferentes mecanismos de identificación. |
| ***8*** | Métodos de Autenticación.  | Analiza los diferentes métodos de autenticación y autorización. | Propicia el trabajo en equipo para implementar mecanismos de autenticación. | Implementa los diferentes mecanismos de autentificación. |
|  | **EVALUACIÓN DE LA UNIDAD DIDÁCTICA** |
| **EVIDENCIA DE CONOCIMIENTO** | **EVIDENCIA DE PRODUCTO** | **EVIDENCIA DE DESEMPEÑO** |
| * Estudio de casos.
* Cuestionarios.
 | * Trabajos individuales y/o grupales.
* Soluciones a ejercicios propuestos.
 | * Comportamiento en clase virtual y chat.
 |

|  |  |
| --- | --- |
| **UNIDAD DIDACTICA III :**  **MECANISMOS DE SEGURIDAD** | **CAPACIDAD DE LA UNIDAD DIDACTICA III:** Propone los mecanismos de seguridad que se pueden implementar en una empresa de acuerdo a su realidad para evitar ataques de intrusos siguiendo recomendaciones internacionales |
| **SEMANA** | **CONTENIDOS** | **ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL** | **INDICADORES DELOGRO DE LA CAPACIDAD** |
| **CONCEPTUAL** | **PROCEDIMENTAL** | **ACTITUDINAL** |
| ***9*** | Contraseñas. Tipos de contraseñas. Administración de contraseñas de usuarios. Políticas de contraseñas.  | Analiza las recomendaciones para la creación y administración de contraseñas.  | Acrecienta el interés sobre la seguridad en la creación y administración de contraseñas.  | **Clase expositiva** (Docente/Alumno)* Uso del Google Meet

**Debate dirigido** (Discusiones)* Foros, chat

**Lecturas*** Uso de repositorios digitales

**Lluvia de ideas (Saberes previos)*** Foros, chat
 | Aplica las principales reglas y políticas para la creación y administración de contraseñas. |
| ***10*** | Biometría. Sistemas Biométricos. Huella digital, Verificación de voz, biometría vascular, Ventajas y desventajas. Bondades. | Analizar los diferentes sistemas biométricos que existen y se pueden implementar en las organizaciones según su realidad. | Se propicia en el estudiante el análisis de los diferentes sistemas biométricos, sus ventajas y desventajas.  | Implementa los diferentes sistemas biométricos, dentro de una organización. |
| ***11*** | Criptografía. Controles criptográficos. Tipos. Certificado digital. Usos y funcionamiento. Ventajas y desventajas. Firma digital. Ventajas y desventajas. Técnicas usadas. | Comprende los diferentes controles criptográficos y su aplicación dentro de las organizaciones. | Se propicia en el estudiante el análisis de los diferentes controles criptográficos y su aplicación dentro de las organizaciones.  | Aplica los diferentes controles criptográficos dentro de las organizaciones. |
| ***12*** | Metodología de ataques informáticos. | Analiza los diferentes métodos de ataques informáticos. | Acrecienta el interés de conocer los diferentes métodos de ataques informáticos.  | Reconoce los diferentes métodos de ataques informáticos.  |
|  | **EVALUACIÓN DE LA UNIDAD DIDÁCTICA** |
| **EVIDENCIA DE CONOCIMIENTO** | **EVIDENCIA DE CONOCIMIENTO** | **EVIDENCIA DE CONOCIMIENTO** |
| * Estudio de casos.
* Cuestionarios.
 | * Trabajos individuales y/o grupales.
* Soluciones a ejercicios propuestos.
 | * Comportamiento en clase virtual y chat.
 |

|  |  |
| --- | --- |
| **UNIDAD DIDACTICA IV :**  **SEGURIDAD EN REDES Y BASES DE DATOS** | **CAPACIDAD DE LA UNIDAD DIDACTICA IV*:*** Evalúa los diferentes tipos de ataques que pueden sufrir sus sistemas de redes y bases de datos, para implementar políticas de seguridad de las mismas de acuerdo a las recomendaciones de normas. |
| **SEMANA** | **CONTENIDOS** | **ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL** | **INDICADORES DELOGRO DE LA CAPACIDAD** |
| **CONCEPTUAL** | **PROCEDIMENTAL** | **ACTITUDINAL** |
| ***13*** | Seguridad en Base de Datos. | Comprende los mecanismos de seguridad dentro de la administración de las bases de datos. | Se propicia en el estudiante el análisis de la importancia de la información que contienen las bases de datos  | **Clase expositiva** (Docente/Alumno)* Uso del Google Meet

**Debate dirigido** (Discusiones)* Foros, chat

**Lecturas*** Uso de repositorios digitales

**Lluvia de ideas (Saberes previos)*** Foros, chat
 | Implementa adecuadamente controles de seguridad en las bases de datos. |
| ***14*** | Seguridad en las redes | Analiza mecanismos de seguridad dentro de la administración de las redes. | Se propicia en el estudiante el análisis de la importancia y seguridad de las redes.  | Implementa adecuadamente controles de seguridad en las redes. |
| ***15*** | Informática forense. | Comprende la importancia y utilización de la informática forense. | Acrecienta el interés sobre el uso de la informática forense.  | Aplica adecuadamente la informática forense. |
| ***16*** | Políticas Informáticas. Ventajas. La ética en la informática. Principios éticos. Los 10 mandamientos de la ética informática.  | Comprende la importancia de implementar políticas de seguridad. | Acrecienta el interés sobre el uso de políticas de seguridad. | Diseña e implementa políticas de seguridad dentro de una organización. |
|  | **EVALUACIÓN DE LA UNIDAD DIDÁCTICA** |  |  |  |
| **EVIDENCIA DE CONOCIMIENTO** | **EVIDENCIA DE CONOCIMIENTO** | **EVIDENCIA DE CONOCIMIENTO** |
| * Estudio de casos.
* Cuestionarios.
 | * Trabajos individuales y/o grupales.
* Soluciones a ejercicios propuestos.
 | * Comportamiento en clase virtual y chat.
 |

**VI. MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDACTICOS**

9

Se utilizarán todos los materiales y recursos requeridos de acuerdo a la naturaleza de los temas programados. Básicamente serán:

**1. MEDIOS Y PLATAFORMAS VIRTUALES:**

* Casos prácticos.
* Pizarra interactiva.
* Google Meet.
* Repositorios de datos.

**2. MEDIOS INFORMÁTICOS:**

* Computadora.
* Tablet.
* Celulares.
* Internet.

**VII. EVALUACION**

La evaluación es inherente al proceso de enseñanza aprendizaje y será continua y permanente. Los criterios de evaluación son de conocimiento, de desempeño y de producto.

1. **EVIDENCIA DE CONOCIMIENTO**

La avaluación será a través de pruebas escritas y orales para el análisis y autoevaluación. En cuanto al primer caso, medir la competencia a nivel interpretativo, argumentativo y propositivo, para ello debemos ver como identifica (describe, ejemplifica, relaciona, reconoce, explica, etc.); y la forma en que argumenta (plantea una afirmación, describe las refutaciones en contra de dicha afirmación, expone sus argumentos contra las refutaciones y llega a conclusiones) y la forma en que propone a través de establecer estrategias, valoraciones, generalizaciones, formulación de hipótesis, respuesta a situaciones, etc.

En cuanto a la autoevaluación permite que el estudiante reconozca sus debilidades y fortalezas para corregir o mejorar.

Las evaluaciones de este nivel serán de respuestas simples y otras con preguntas abiertas para su argumentación.

1. **EVIDENCIA DE DESEMPEÑO**

Esta evidencia pone en acción recursos cognitivos, recursos procedimentales y recursos afectivos; todo ello en una integración que evidencia un saber hacer reflexivo; en tanto, se puede verbalizar lo que se hace, fundamentar teóricamente la práctica y evidenciar un pensamiento estratégico, dado en la observación en torno a cómo se actúa en situaciones impredecibles.

La evaluación de desempeño se evalúa ponderando como el estudiante se hace investigador aplicando los procedimientos y técnicas en el desarrollo de las clases a través de su asistencia y participación asertiva.

1. **EVIDENCIA DE PRODUCTO**

Están implicadas en las finalidades de la competencia, por tanto, no es simplemente la entrega de producto, sino que tiene que ver con el campo de acción y los requerimientos del contexto de aplicación.

La evaluación de producto se evidencia en la entrega oportuna de sus trabajos.

Además, se tendrá en cuenta la asistencia como componente del desempeño, el 30% de inasistencia inhabilita el derecho de evaluación.

|  |  |  |
| --- | --- | --- |
| **VARIABLES** | **PONDERACIONES** | **UNIDADES DIDÁCTICAS DENOMINADAS MODULOS** |
|  Evaluación de Conocimiento | 30 % | El ciclo académico comprende de 4 |
|  Evaluación de Producto | 35 % |
|  Evaluación de Desempeño | 35 % |

Siendo el promedio final (PF), el promedio simple de los promedios ponderados de cada módulo (PM1, PM2, PM3, PM4).

$$PF = \frac{PM1 +PM2+PM3+PM4}{4}$$

Para aprobar el curso se requiere de una nota mínima de 10,5 puntos.

**VIII. BIBLIOGRAFIA**

* 1. **Fuentes Documentales**
* DIRECCION GENERAL DE MODERNIZACION ADMINISTRATIVA, PROCEDIMIENTOS EIMPULSO DE LA ADMINISTRACION ELECTRONICA. (2012). Metodología de análisis y gestión de riesgos de los sistemas de información versión 3.0. España: Ministerio de Hacienda y Administraciones Públicas
	1. **Fuentes Bibliográficas**
* Garcia, A. (2011). Seguridad Informática.
* López, I. (2014). Gestión de Bases de Datos
* McCarthy. Seguridad Digital. Mc. Graw-Hill.
* MITNICK, K., SIMON W. (2008). El Arte de la Intrusion - Como Ser un Hacker o Evitarlos (Spanish Edition). España:Ra-MA
* MITNICK, K., SIMON W. (2005). The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers. USA: Wiley Publishing.
* MITNICK, K., SIMON W. (2003). The Art of Deception: Controlling the Human Element of Security. USA: Wiley Publishing.
* Piattini, M. y De Peso, E. (2001). AUDITORIA INFORMATICA – Un enfoque práctico. RA-MA Editorial.
* Raya. Seguridad de una Red Netware. (5ta. Ed. ) Alfaomega.
	1. **Fuentes Electrónicas**
* Metodología de Análisis y Gestión de Riesgos de los sistemas de información, MAGERIT versión 3.0. <https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/>
* Norma Técnica Peruana NTP ISO 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información. INDECOPI, 2007. http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf
* Norma Técnica Peruana NTP ISO 27001:2014. Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición. http://portal.indecopi.gob.pe/cidalerta/buscadocdet.aspx?id=21374
* Recursos de Seguridad de la Información. http://www.isaca.org - http://www.sans.org - http://www.intypedia.com/ - http://www.welivesecurity.com/la-es

Huacho, Junio del 2020

Universidad Nacional

“José Faustino Sánchez Carrión”

……………………………………..

Mg. Barrera Loza, Ana Doris Magdalena

**DNU 185**

10