VI. MEDIOS Y MATERIALES

MEDIOS: Pizarra, proyector multimedia y computadora
MATERIALES: Separatas, archivos personales e Internet.

VII. EVALUACIÓN.

DIAGNOSTICA: Sustentación oral de un tema actual.
FORMATIVA: Será permanente durante el proceso Enseñanza-Aprendizaje y según los criterios de evaluación con participación en forma individual o grupal, en sus aprendizajes, que permitan tomar las acciones de retroalimentación para alcanzar las competencias programadas. Observación personal y/o en equipo.
Las calificaciones y promedios están de acuerdo a los artículos del 121º al 146º del Reglamento Académico General aprobado con Resolución de C.U. N° 0130-2015- CU-UNJFSC, del 20/Febrero/2015.

Promedio Parcial = Evaluación Escrita + Evaluación Oral + Trabajo Académico

El Promedio Final es: **PF = (P1 + P2) / 2**

VIII. BIBLIOGRAFÍA.

1. William Stalling Comunicaciones y Redes de Computadoras
2. Mario G.Piattini / Emilio de Peso AUDITORIA INFORMATICA – Un enfoque práctico RA-MA Editorial, 2001
3. Alvaro Gómez (2013). Seguridad en equipos informáticos.
4. Alfonso Garcia (2011). Seguridad Informática.

Mg. Ana Doris M. Barrera Loza
Catedrático del Curso

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRION
Facultad de Ingeniería Industrial, Sistemas e Informática

ASIGNATURA: Seguridad de la Información

I. DATOS GENERALES.

1.1.	CÓDIGO	: 504
1.2.	ESCUELA PROFESIONAL	: Ingeniería Informática
1.3.	DEPARTAMENTO ACADEM.	: Ingeniería
1.4.	CICLO DE ESTUDIOS	: IX
1.5.	CRÉDITOS	: 3.0
1.6.	CONDICIÓN	: Obligatorio
1.7.	HORAS SEMANALES	: 04
1.8.	HORAS TEÓRICAS	: 02
1.9.	HORAS DE PRÁCTICA	: 02
1.10.	PRE-REQUISITO	: 453 – Form. y Eval. de Proy. inform
1.11.	SEMESTRE ACADÉMICO	: 2018-I
1.12.	DOCENTE	: Mg. Ana Doris M. Barrera Loza
		anadobar@hotmail.com

II. SUMILLA.

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.

III. OBJETIVOS.

Diseñar el plan de seguridad que debería adoptarse 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.

IV. PROGRAMACIÓN DE CONTENIDOS.

4.1 UNIDAD TEMÁTICA I. INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

SEMANA I

Introducción a la seguridad de la Información. Principios. Seguridad física y lógica. Calidad de la información. Seguridad informática. Objetivos. Áreas. Mecanismos de Seguridad. Causas de la inseguridad.

SEMANA II

Activos. Amenazas. Vulnerabilidad. Riesgo e impacto en los negocios.

SEMANA III

Gestión de la Seguridad de la Información. Beneficios. Ciclo de Deming. Planificar y Hacer. Alcance. Inventario de Activos.

SEMANA IV

Gestión de la Seguridad de la Información. Gestión de riesgos. Análisis de riesgos. Tratamiento de riesgos. Declaración de aplicabilidad. Implementación del SGSI. Revisar y actuar.

4.2 UNIDAD TEMÁTICA II. CONTROL DE ACCESOS

SEMANA V

Serie Norma ISO 27000. ISO 27001. Beneficios. Implementación. Certificación.

SEMANA VI

Control de Accesos. Temas. Principios. Acceso. Sujeto, Objeto. MR. Categorías de control de Acceso: Administrativo, Lógico, Físico. Control de Acceso Preventivo, Detectivo, Correctivo, Disuasivos, de Recuperación y Compensatorios.

SEMANA VII

Técnicas de control de accesos. Tipos de control de acceso. Identificación, Autenticación, Autorización. Métodos de Autenticación: Algo que se sabe. Algo que se tiene, Algo que se es. Otros mecanismos de Identificación y Autenticación.

SEMANA VIII: Primer Examen Parcial.

4.3 UNIDAD TEMÁTICA III. MECANISMOS DE SEGURIDAD Y ATAQUES

SEMANA IX

Contraseñas. Debiles y fuertes. Tipos de contraseñas: estáticas, dinámicas, Passphrase. Administración de contraseñas de usuarios. Políticas de contraseñas. Consejos a seguir. Métodos de ataques a contraseñas: Ataques de Fuerza Bruta, Ataques de Diccionario. Ingeniería Social.

SEMANA X

Biometría. Sistemas Biométricos. Huella digital, Verificación de voz, Verificación de patrones oculares, Geometría de la mano, Biometría vascular. Ventajas y desventajas. Bondades.

SEMANA XI

Criptografía. Controles criptográficos. Tipos. Certificado digital. Usos y funcionamiento. Ventajas y desventajas. Firma digital. Ventajas y desventajas. Técnicas usadas.

SEMANA XII

Ataques informáticos.

4.4 UNIDAD TEMÁTICA IV. SEGURIDAD EN REDES

SEMANA XIII

Seguridad en Base de Datos. Seguridad en las redes.

SEMANA XIV

Informática forense.

SEMANA XV

Políticas Informáticas. Ventajas. Políticas sobre la asignación y uso de recursos. Políticas sobre actualización de equipos. Políticas sobre la seguridad de la información. Políticas sobre el mantenimiento y el buen uso de la infraestructura. Políticas sobre la capacitación del recurso humano. La ética en la informática. Principios éticos. Los 10 mandamientos de la ética informática. Nuevas tecnologías de informaci´n y vacío legal.

SEMANA XVI

Segundo Examen Parcial

SEMANA XVII

Examen Sustitutorio

V. METODOLOGÍA.

Se utilizará el método Heurístico (como resultado de la experiencia) para obtener una solución que se ajuste a casos reales. Se presentarán conceptos, métodos y técnicas que permitan planificar, desarrollar y administrar aplicaciones informáticas para la empresa haciendo énfasis en aplicaciones concretas, y donde, el Profesor compartirá sus experiencias profesionales.