PROGRAMA DE ASIGNATURA - SÍLABO

1. DATOS GENERALES

Modalidad: PRESENCIAL ESPE LTGA-G RODRIGUEZ LARA	**Departamento:** CIENCIAS DE LA COMPUTACION		**Área de Conocimiento:** DISEÑO Y ADM DE REDES	
Nombre Asignatura: GEST. SEG. TEC. INFORMACION	**Período Académico:** PREGRADO S-II OCT21-MAR22			
Fecha Elaboración: 30/11/20 05:57 PM	**Código:** L0I03	**NRC:** 9042		**Nivel:** PREGRADO
Docente: CASA GUAYTA CARLOS WELINGTON cwcasa@espe.edu.ec				

Unidad de Organización	PROFESIONAL
Campo de Formación:	FUNDAMENTOS TEÓRICA
Núcleos Básicos de	Seguridad. Seguridad de la infraestructura. Ciberseguridad.

CARGA HORARIA POR COMPONENTES DE APRENDIZAJE			**SESIONES SEMANALES**
DOCENCIA	**PRACTICAS DE APLICACIÓN Y EXPERIMENTACIÓN**	**APRENDIZAJE AUTÓNOMO**	2
32	32	32	

Fecha Elaboración	**Fecha de Actualización**	**Fecha de Ejecución**
27/11/2020	27/11/2020	30/11/2020

Descripción de la Asignatura:

Gestión de la Seguridad en Tecnologías de la Información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Contribución de la Asignatura:

La asignatura de Gestión de la Seguridad en Tecnologías de la Información permitirá a los estudiantes de Tecnología en Redes y Telecomunicaciones, acceder a la información y los procesos que la apoyan, los sistemas y las redes, son bienes importantes de las entidades, por lo que requieren ser protegidos convenientemente frente a amenazas que pongan en peligro la disponibilidad, la integridad, la confidencialidad de la información, la estabilidad de los procesos, los niveles de competitividad.

Resultado de Aprendizaje de la Carrera: (Unidad de Competencia)

Identifica potenciales vulnerabilidades de seguridad y aplica métodos correctivos para garantizar la integridad de la información

Objetivo de la Asignatura: (Unidad de Competencia)

Formar profesionales de nivel Tecnológico Superior en Redes y Telecomunicaciones, mediante el desarrollo de competencias que permitan solucionar problemas de conectividad utilizando las tecnologías de la información y comunicación, para garantizar la integridad, confidencialidad y disponibilidad de la información

Resultado de Aprendizaje de la Asignatura: (Elemento de Competencia)

Identifica potenciales vulnerabilidades de seguridad y aplica métodos correctivos para garantizar la integridad de la información

PROGRAMA DE ASIGNATURA - SÍLABO

Proyecto Integrador

Aplica a Tecnologías de la Información.

PERFIL SUGERIDO DEL DOCENTE

TÍTULO Y DENOMINACIÓN

GRADO: Ingeniero de Sistemas e Informática, Ingeniero en Computación, Ingeniero en Ciencias de la Computación

POSGRADO: Gestión de la Información y Tecnologías de la Comunicación

2. SISTEMA DE CONTENIDOS Y RESULTADOS DEL APRENDIZAJE

CONTENIDOS		
Unidad 1 **Horas/Min:** 22:00 Seguridad	**HORAS DE TRABAJO AUTÓNOMO** Prácticas de Aplicación y Experimentación	
Amenazas a la seguridad 1.1 Amenazas a la seguridad 1.2 Política de seguridad 1.3 Conceptos de seguridad en redes 1.4 Conceptos básicos de seguridad informática 1.5 Legislación nacional e internacional relacionada con la seguridad de la información	**Tarea 1**	INVESTIGAR SOBRE AMENAZAS A LA SEGURIDAD
Enfoque integral de la seguridad de la información 1.6 Enfoque integral de la seguridad de la información 1.7 Encriptación 1.8 Detección de intrusión y respuesta ante una brecha de seguridad 1.9 Sistemas de detección de intrusos de red (NIDS). 1.10 Firewall 1.11 Gestión de riesgos. Análisis de riesgos de tecnología de información	**Laboratorio 1**	REALIZAR DETECCIÓN DE INTRUSIÓN Y RESPUESTA ANTE UNA BRECHA DE SEGURIDAD
Análisis de vulnerabilidades 1.12 Análisis de vulnerabilidades 1.14 Información de seguridad y gestión de eventos Control de Accesos 1.15 Objetivos del Control de Acceso. 1.16 Principios del Control de Acceso. 1.17 Pasos para UN CONTROL DE Acceso. 1.18 Tipos de Control de Acceso. 1.19 Gestión de Accesos a usuarios. 1.20 Control de Accesos al Sistema Operativo.	**Tarea 2**	INFORMACIÓN DE SEGURIDAD Y GESTIÓN DE EVENTOS CONTROL DE ACCESOS
Métodos de Control de Acceso 1.21 Métodos de Control de Acceso. 1.22 Ingeniería social. 1.24 Protecciones contra los ataques de ingeniería social	**Laboratorio 2**	REALIZAR MÉTODOS DE CONTROL DE ACCESO.

PROGRAMA DE ASIGNATURA - SÍLABO

2. SISTEMA DE CONTENIDOS Y RESULTADOS DEL APRENDIZAJE

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTES DE DOCENCIA	10
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	12
HORAS DE TRABAJO AUTONOMO	10
TOTAL HORAS POR UNIDAD	**32**

CONTENIDOS		
Unidad 2 **Horas/Min:** 20:00 Seguridad de la infraestructura	**HORAS DE TRABAJO AUTÓNOMO** Prácticas de Aplicación y Experimentación	
SEGURIDAD DE PUESTOS DE USUARIO 2.1 SEGURIDAD DE PUESTOS DE USUARIO 2.2 PROTECCIÓN DE SISTEMAS CRÍTICOS **PROTECCIÓN DE REDES** 2.3 PROTECCIÓN DE REDES 2.4 PROTECCIÓN DE SERVICIOS EN LA NUBE 2.5 MONITORIZACIÓN Y GESTIÓN DE INCIDENTES 2.6 GESTIÓN DE IDENTIDADES. 2.7 GESTIÓN DE VULNERABILIDADES 2.9 PROTECCIÓN DE APLICACIONES **Malware** 2.10 Malware. 2.11 Criptografía 2.12 Evaluación de la seguridad de un sistema criptográfico 2.13 Formas de romper la seguridad **Seguridad condicional** 2.14 Seguridad condicional 2.15 La criptografía en el correo electrónico 2.16 Seguridad de Infraestructura y redes	**Tarea 1** **Laboratorio 1** **Tarea 2** **Laboratorio 2**	investigacion SEGURIDAD DE PUESTOS DE USUARIO PROTECCIÓN DE SERVICIOS EN LA NUBE investigacion sobre MALWARE. LA CRIPTOGRAFÍA EN EL CORREO ELECTRÓNICO

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTES DE DOCENCIA	10
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	12
HORAS DE TRABAJO AUTONOMO	10
TOTAL HORAS POR UNIDAD	**32**

CONTENIDOS		
Unidad 3 **Horas/Min:** 22:00 Ciberseguridad	**HORAS DE TRABAJO AUTÓNOMO** Prácticas de Aplicación y Experimentación	
Amenazas 3.1 Amenazas de Internet **Ataques** 3.2 Ataques a sitios web 3.3 Ataques a aplicaciones web 3.4 Ataque DDoS (Distributed Denial of Service)	**Tarea 1**	investigue AMENAZAS DE INTERNET

PROGRAMA DE ASIGNATURA - SÍLABO

2. SISTEMA DE CONTENIDOS Y RESULTADOS DEL APRENDIZAJE

Investigación bibliográfica botnet		
3.5 Botnets		
3.6 Phishing		
3.7 Spam.		
3.8 Ransomware		
3.9 Cibercrimen		
3.10 Ayuda a los spammers		
3.11 Ataques a la red distribuidos/DDoS	**Tarea 2**	investigue ATAQUES A LA RED DISTRIBUIDOS/DDOS
3.12 Qué es un botnet		
3.13 Llamadas con tarificación especial y envío de SMS de pago		
3.14 Robo de dinero electrónico		
3.15 Robo de datos bancarios online		
3.16 Ransomware y ciberchantaje		
Virus		
3.17 Evolución de los métodos de propagación de virus3.17		
3.17.1 Estado del arte de la interfaz del sistema operativo		
3.18. Configuración del sistema operativo en RED.	**Laboratorio 1**	CONFIGURACIÓN DEL SISTEMA OPERATIVO EN RED.
3.18.1 Requerimientos al instalar una RED	**Laboratorio 2**	REQUERIMIENTOS AL INSTALAR UNA RED

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTES DE DOCENCIA	10
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	12
HORAS DE TRABAJO AUTONOMO	10
TOTAL HORAS POR UNIDAD	**32**

Empleo de Tics en los Procesos de Aprendizaje	
1	Herramientas Colaborativas (Google, drive, onedrives, otros)
2	Software de Simulación
3	Aula Virtual

4. RESULTADOS DEL APRENDIZAJE, CONTRIBUCIÓN AL PERFIL DEL EGRESO Y TÉCNICA DE

PROYECTO INTEGRADOR DEL NIVEL RESULTADO DE APRENDIZAJE POR UNIDAD CURRICULAR	**Niveles de logro: Alta(A), Media (B), C(Baja).**	**ACTIVIDADES INTEGRADORAS**
1. Describe las normativas legales sobre la Ciberseguridad, las amenazas de internet.	Alta A	INVESTIGAR LOS PRINCIPIOS BASICOS DE LA SEGURIDAD INFORMATICA
2. Describe los principios básicos de la Seguridad de la Información, las amenazas a la seguridad, implementando medidas efectivas para el control de las mismas.	Alta A	VERIFICAR QUE POLITICAS DE SEGURIDAD SE PUEDE UTILIZAR EN LA SEGURIDAD INFORMATICA

PROYECTO INTEGRADOR DEL NIVEL RESULTADO DE APRENDIZAJE POR UNIDAD CURRICULAR	Niveles de logro: Alta(A), Media (B), C(Baja).	ACTIVIDADES INTEGRADORAS
3. Realiza un análisis de las políticas de seguridad, así como la legislación nacional e internacional relacionada con la seguridad de la información.	Alta A	DESARROLLAR E INVESTIGAR LOS REQUISITOS DE LA SEGURIDAD INFORMATICA
4. Describe los requisitos para aplicar la seguridad de la Infraestructura.	Alta A	ANALIZAR LA PROTECCIÓN DE LOS SISTEMAS CRITICOS DE LA SEGURIDAD INFORMATICA
5. Describe y analiza la protección de sistemas críticos, la protección de redes informáticas y la protección de servicios en la nube.	Alta A	DESARROLLAR LAS NORMATIVAS LEGALES SOBRE CIBERSEURIDAD
6. Identifica los pasos para la implementación de un plan de seguridad para evitar los ataques a sitios web.	Alta A	IMPLEMENTAR UN PLAN DE CONTINGENCIA DE SEGURIDAD INFORMATICA

6. TÉCNICAS Y PONDERACION DE LA EVALUACIÓN

Técnica de evaluación	1er Parcial	2do Parcial	3er Parcial
Investigación Bibliográfica	4	4	4
Pruebas oral/escrita	6	6	6
Laboratorios/Informes	4	4	4
Examen Parcial	6	6	6
TOTAL:	**20**	**20**	**20**

7. BIBLIOGRAFÍA BÁSICA/ TEXTO GUÍA DE LA ASIGNATURA

Titulo	Autor	Edición	Año	Idioma	Editorial
Auditoría de seguridad informatica	Gómez Vieites	-	2013	Español	Bogotá : Ediciones de la U
Auditoría Informática : un enfoque práctico	Piattini Velthuis, Mario Gerardo	2	2001	spa	Alfaomega
Reingeniería de la Auditoría Informática	Solís Montes, Gustavo Adolfo		2002	spa	Trillas

8. BIBLIOGRAFÍA COMPLEMENTARIA

Titulo	Autor	Edición	Año	Idioma	Editorial
CEH Certified Ethical Hacker Allin-One Exam Guide CEH Certified Ethical Hacker All-in-One Exa	MATT WALKER	4	2019	ingles	MC GRAWLL HILL

9. LECTURAS PRINCIPALES

Tema	Texto	Página	URL

Tema	Texto	Página	URL
Tipos de seguridad informática más importantes a conocer y tener en cuenta	OBS BUSINESS		https://obsbusiness.school/int/bloginvestigacion/sistemas/tiposde- seguridad-informatica-masimportantes-conocer-y-teneren- cuenta

10. ACUERDOS

Del Docente:

1 Esforzarme en conocer con amplitud al campo académico y práctico

2 Asistir a clases siempre y puntualmente dando ejemplo al estudiante para exigirle igual comportamiento

3 Mantener en todo momento un clima de empatía y consideración entre estudiantes, profesores, administrativos, trabajadores, etc.

4 Cumplir con las leyes y reglamentos institucionales y orientar todos los esfuerzos en la dirección de los grandes propósitos de la Universidad (Misión, Visión)

De los Estudiantes:

1 Ser honesto, no copiar, no mentir

2 Firmar toda prueba y trabajo que realizo en conocimiento que no he copiado de fuentes no permitidas

3 Cumplir con las leyes y reglamentos institucionales y orientar todos los esfuerzos en la dirección de los grandes propósitos de la Universidad (Misión, Visión)

4 Cumplir con las obligaciones de estudiantes y docentes para devengar la inversión que hace el estado Ecuatoriano en favor de los mismos.

FIRMAS DE LEGALIZACIÓN

CARLOS WELINGTON CASA GUAYTA

Firmado digitalmente por CARLOS WELINGTON CASA GUAYTA
Fecha: 2022.02.25 11:29:03 -05'00'

FIRMADO Y SELLADO

CARLOS WELINGTON CASA GUAYTA
DOCENTE

LUIS ALBERTO GUERRA CRUZ
COORDINADOR DE AREA DE CONOCIMIENTO

LUCAS ROGERIO GARCES GUAYTA
DIRECTOR DE DEPARTAMENTO