



FACULTAD EN REDES Y TELECOMUNICACIONES
IER910/Seguridad de Redes
Período: 2016 - 2

1. Identificación.-

Número de sesiones: 48

Número de horas: 120 (48 presencial + 72 de trabajo autónomo)

Créditos: 3

Profesor: William Villegas

Correo electrónico del docente (Udlanet): w.villegas@udlanet.ec

Coordinador: Angel Jaramillo

Campus: Queri

Pre-requisito: Co-requisito:

Paralelo: 2

Tipo de asignatura:

| | |
|-------------|---|
| Optativa | |
| Obligatoria | X |
| Práctica | |

Organización unidad curricular:

| | |
|---------------------------------|---|
| Unidad 1: Formación Básica | |
| Unidad 2: Formación Profesional | X |
| Unidad 3: Titulación | |

Campo de formación:

| Campo | | | | |
|----------------------|--------------------|---|---|--------------------------|
| Fundamentos teóricos | Praxis profesional | Epistemología y metodología de la investigación | Integración de saberes, contextos y cultura | Comunicación y lenguajes |
| | X | | | |

2. Descripción del curso.-

Seguridad de redes es una materia que aborda el estudio de los diversos conceptos de seguridad en una red y su aplicación para mantener la integridad, disponibilidad y confidencialidad de la información y los equipos dentro de la red, utilizando herramientas y metodologías de medición así como del levantamiento



de la información para su análisis con el fin de inferir criterios y recomendaciones para la seguridad de redes.

3. Objetivo del curso.-

Analizar con fundamento los criterios y componentes de seguridad de una red para su implementación en casos reales.

4. Resultados de aprendizaje deseados al finalizar el curso:

| Resultados de aprendizaje | RdA perfil de egreso de carrera | Nivel de dominio (carrera) |
|---|---|--|
| | Electrónica y redes de Información | |
| <ol style="list-style-type: none">1. Identifica los conceptos relacionados con la seguridad de la información en una organización2. Evalúa criterios que garanticen el aseguramiento de la información de una infraestructura tecnológica. | Gestiona la seguridad en redes, a través de la selección y la configuración de los componentes de software y hardware, en función de los requerimientos de la organización. | Inicial () Medio () Final (X) |
| | Redes y telecomunicaciones | |
| | 4. Gestiona adecuadamente la seguridad en redes, seleccionando los componentes de hardware y software y configurando sus parámetros necesarios en función de los requerimientos de la organización. | |

5. Sistema de evaluación.-

De acuerdo al Modelo Educativo de la UDLA la evaluación busca evidenciar el logro de los resultados de aprendizaje (RdA) enunciados en cada carrera y asignatura, a través



de mecanismos de evaluación (MdE). Por lo tanto la evaluación debe ser continua, formativa y sumativa.

Es necesario recordar que cada reporte de Progreso (1 y 2 respectivamente) debe contemplar diversos MdE, como: proyectos, exámenes, análisis de caso, portafolio, ejercicios, entre otros. Sin embargo, **ninguna evaluación individual podrá tener más del 20% de la ponderación total de cada reporte de evaluación**. Asimismo, se usará la rúbrica basada en criterios para la evaluación y retroalimentación, que será entregada al estudiante previamente para que tenga claras indicaciones de cómo va a ser evaluado. Además toda asignatura tendrá **un mecanismo específico de evaluación final (proyecto o examen) con su ponderación específica (la evaluación final puede tener 1 o 2 componentes = 30% del total)**.

Al finalizar el curso habrá un examen de recuperación para los estudiantes que deseen reemplazar la nota de un examen anterior (ningún otro tipo de evaluación). Este examen es de carácter complejo y de alta exigencia, por lo que el estudiante necesita prepararse con rigurosidad. La nota de este examen reemplazará a la del examen que sustituye. Para rendir el **Examen de Recuperación**, es requisito que el estudiante **haya asistido por lo menos al 80%** del total de las sesiones programadas de la materia.

Asistencia: Es obligatorio tomar asistencia en cada sesión de clase.

La UDLA estipula la siguiente distribución porcentual para los reportes de evaluaciones previstas en cada semestre de acuerdo al calendario académico:

| | |
|------------------------|-----|
| Reporte de progreso 1: | 35% |
| Reporte de progreso 2: | 35% |
| Evaluación final: | 30% |

6. Metodología del curso y de mecanismos de evaluación.-

De acuerdo al modelo educativo de la UDLA, la metodología que se utilizará durante todo el curso, debe estar centrada principalmente en el estudiante (aprendizaje), con enfoque constructivista a través de la participación constante, el trabajo cooperativo y la permanente vinculación entre la teoría y la práctica.

Los temas tratados en cada clase contarán con la participación activa del estudiante y la asistencia del docente a través de la socialización de los sílabos por resultados de aprendizaje, clases magistrales, micro ensayos y talleres que evidencien el trabajo colaborativo de los estudiantes, los mismos que serán reforzados con lecturas y cuestionarios de documentos pertinentes a cada unidad temática.

Para afianzar el conocimiento adquirido, se realizarán prácticas de laboratorio. Para cada práctica de laboratorio los alumnos deberán realizar previamente un trabajo preparatorio



utilizando una Guía de Prácticas de Laboratorio que le proporciona el docente a través de la plataforma virtual. Durante las prácticas de laboratorio los estudiantes verificarán los resultados obtenidos en su trabajo preparatorio, luego de lo cual registrarán sus observaciones en un informe, con el respectivo análisis de resultados, evidencia multimedia, conclusiones y anexos evidenciados en un informe con el formato de la IEEE que será subido al repositorio de prácticas de laboratorio en la plataforma virtual.

En progreso 1 y 2 (35% cada uno):

- **Resumen de Documentos** – 4%: El estudiante debe leer el documento planteado y resumir utilizando organizadores gráficos por cada tema y compartirlos en la plataforma virtual. (Se adjunta rúbrica).
- **Resolución de Cuestionarios** – 4%: El estudiante debe contestar las preguntas planteadas por cada tema y compartirlos en la plataforma virtual. (Se adjunta rúbrica).
- **Portafolio** - 7%: Portafolio de prácticas de laboratorio con un informe bajo el formato de la IEEE.
- **Prueba** – 20%: El estudiante rendirá una evaluación teórica y de resolución de problemas al finalizar cada RdA. (Se adjunta rúbrica).

Evaluación final:

- **Proyecto** – 20%,
- **Examen final** – 10%: Son preguntas de elección múltiple y resolución de ejercicios que implican el estudio **de toda la asignatura**.

7. Temas y subtemas del curso.-

| RDA | Temas | Subtemas |
|--|---|--|
| 1. Identifica los conceptos relacionados con la seguridad de la información en una organización. | 1. Amenazas de seguridad en las redes modernas | 1.1. Principios fundamentales de las redes seguras 1.2. Gusanos, virus y troyanos 1.3. Metodologías de ataque |
| | 2. Asegurando dispositivos de red | 2.1. Asegurando el acceso y los ficheros de los dispositivos 2.2. CLI basada en roles 2.3. Dispositivos de monitorización 2.4. Utilización de características automatizadas |

| | | |
|---|---|--|
| | 3. Autenticación, autorización y contabilidad | 3.1. Propósito de AAA |
| | 4. Implementación de tecnologías de cortafuegos | 4.1. Listas de control de acceso 4.2. Tecnologías de cortafuegos. 4.3. Control de acceso basado en contexto 4.4. Políticas de cortafuegos |
| | 5. Implementación de la prevención de la intrusión | 5.1. Tecnologías IPS 5.2. Implementación de IPS |
| 2. Evalúa criterios que garanticen el aseguramiento de la información de una infraestructura tecnológica. | 6. Asegurando la red de área local | 6.1. Consideraciones finales de seguridad 6.2. Consideraciones de seguridad de capa 2 6.3. Wireless, VoIP y consideraciones de seguridad SAN 6.4. Configuración de la seguridad del switch 6.5. SPAN y RSPAN |
| | 7. Criptografía | 7.1. Servicios criptográficos 7.2. Resúmenes, firmas digitales y autenticación 7.3. Encriptación simétrica y asimétrica |
| | 8. Implementación de las redes privadas virtuales | 8.1. VPNs 8.2. Componentes y operaciones de las VPNs IPSEC 8.3. Implementación de VPNs site-to-site. 8.4. Implementación de VPNs de acceso remoto 8.5. Implementación de SSLVPNs |
| | 9. Gestionar una red | 9.1. Ciclo de vida de una red |



| | | |
|--|--|--|
| | segura | segura 9.2. Red de autodefensa |
| | 10. Crear e implementar una política de seguridad de una red. | 10.1 Crear e implementar una política de seguridad de una red. |

8. Planificación secuencial del curso.-

| Semana 1-5 | | | | | |
|------------|---|--|--|--|---|
| # RdA | Tema | Sub tema | Actividad/ metodología/clase | Tarea/ trabajo autónomo | MdE/Producto/ fecha de entrega |
| 1 | 1. Amenazas de seguridad en las redes modernas | 1.1. Principios fundamentales de las redes seguras 1.2. Gusanos, virus y troyanos 1.3. Metodologías de ataque | Introducción: Normas del curso Presentación magistral: Amenazas de seguridad en las redes modernas Taller | Lectura Documento 1 | Repositorio resumen Documentos (rúbrica) |
| 1 | 2. Asegurando dispositivos de red | 2.1. Asegurando el acceso y los ficheros de los dispositivos 2.2. CLI basada en roles 2.3. Dispositivos de monitorización 2.4. Utilización de características automatizadas | Presentación magistral: Taller Portafolio de prácticas de Laboratorio No1 | Lectura Documento 2 Informes de Práctica de laboratorio No1 | Repositorio resumen Documentos (rúbrica) Repositorio Informes Laboratorios (rúbrica) |

| 1 | 3. Autenticación, autorización y contabilidad | 3.1. Propósito de AAA | Presentación magistral: Taller Portafolio de prácticas de Laboratorio No2 | Lectura Documento 3 Informes de Práctica de laboratorio No2 | Repositorio resumen Documentos (rúbrica) Repositorio Informes Laboratorios (rúbrica) Repositorio de laboratorios, Control de lectura y Talleres: 15% Examen Progreso 1 Quinta semana (Paralelo 1) Quinta semana (Paralelo 2) 20% |
|-------------|--|---|---|--|---|
| Semana 6-10 | | | | | |
| # RdA | Tema | Sub tema | Actividad/ metodología/clase | Tarea/ trabajo autónomo | MdE/Producto/ fecha de entrega |
| 1 | 4. Implementación de tecnologías de cortafuegos | 4.1. Listas de control de acceso 4.2. Tecnologías de cortafuegos 4.3. Control de acceso basado en contexto 4.4. Políticas de cortafuegos | Presentación magistral: Taller Portafolio de prácticas de Laboratorio No3 | Lectura Documento 4 Informe de Práctica de laboratorio No3 | Repositorio resumen Documentos (rúbrica) Repositorio Informes Laboratorios (rúbrica) |
| | 5. Implementación de la prevención de la intrusión | 5.1. Tecnologías IPS 5.2. Implementación de IPS | Presentación magistral: Portafolio de prácticas de Laboratorio No4 | Lectura Documento 5 Informe de Práctica de laboratorio No4 | Repositorio resumen Documentos (rúbrica) Repositorio Informes Laboratorios (rúbrica) |
| | 6. Asegurando la red de área local | 6.1. Consideraciones finales de seguridad | | | |





| | | | | | |
|---|---|---|---------------------------------------|----------------------|--|
| 2 | 9. Gestionar una red segura | 9.1. Ciclo de vida de una red segura 9.2. Red de autodefensa | Presentación magistral: Taller | Lectura Documento 9 | Repositorio resumen Documentos (rúbrica) |
| 2 | 10. Crear e implementar una política de seguridad de una red. | 10.1 Crear e implementar una política de seguridad de una red. | Presentación magistral: Taller | Lectura Documento 10 | Repositorio resumen Documentos (rúbrica) <hr/> Proyecto Final 20% Semana 15 (Paralelo 1) Semana 15 (Paralelo 2) Examen final 10% Semana 16 (Paralelo 1) Semana 16 (Paralelo 2) |

9. Observaciones generales.-

Se pone a disposición del estudiante la información relevante de cada una de las actividades desarrolladas a lo largo del curso a través del aula virtual: SEGURIDAD DE REDES de la página de la universidad.

Se debe considerar que cuando se trata de un resumen de un capítulo, este tiene que ser realizado utilizando herramientas como mapas mentales, organizadores gráficos, cuadros sinópticos, etc. y subido a la plataforma virtual en el plazo establecido.

Todos los informes y trabajos autónomos, deben ser realizados utilizando el formato adecuado y siempre deben incluir las fuentes de información, las mismas que han de ser citadas de acuerdo a las normas APA.

Ninguna evaluación, trabajo o proyecto será considerado fuera del plazo establecido.



No se permite el ingreso y mucho menos el consumo de ninguna clase de alimento ni bebida en la sala de clase. Esto es aún más crítico si la clase se desarrolla en un laboratorio.

Se considerará como asistencia si el estudiante arriba a la sala de clase dentro de los primeros diez minutos de la hora de clase. Si el estudiante llega pasados los diez primeros minutos de iniciada la hora de clase, automáticamente se registra su falta.

No está permitido ningún tipo de trato irrespetuoso, discriminatorio, descortés, etc. hacia los compañeros o el docente. En caso de cometer alguna de estas faltas, el docente se reserva el derecho de aplicar una sanción de acuerdo a la gravedad del hecho.

10. Referencias bibliográficas.-

- CCNA SECURITY. Módulos 1 a 10, Recuperado el 8 de septiembre de 2014 de <http://cisco.netacad>.
- Stallings, W. (2011). *Cryptography and network security*. Boston, MA: Prentice Hall.

10.1 Referencias complementarias.-

Tanenbaum, A. (1997). *Redes de Computadores*. México. Printece-Hall

11. Perfil del docente.

William Villegas

Magister en redes de comunicaciones (Pontificia Universidad Católica del Ecuador), Ingeniero de sistemas con mención en Robótica e inteligencia Artificial (Universidad politécnica Salesiana). 10 años en el campo empresarial, 6 años de experiencia en sistemas en el Área de redes e infraestructura, 5 años de experiencia en el campo de la educación.

Contacto: w.villegas@udlanet.ec

Oficina: Bloque 7, segundo piso, puesto 8.

Horario de atención al estudiante: lunes a jueves desde 15:00 – 17:00