PROGRAMA DE ESTUDIOS:

CURSO DE SEGURIDAD DE REDES Y EN LA NUBE

KOICA HANDONG GLOBAL UNIVERSITY CIT UNA

Seguridad de Redes y en la Nube

Información Básica

Información del curso

1. Título: **Seguridad de Redes y en la Nube**
2. Año lectivo: **2024**
3. Semestre: **Primero**
4. Departamento: **Centro de Innovación TIC (FP-UNA)**
5. Año/Nivel: **Intermedio**
6. Formato de clase: **Clases interactivas y sesiones prácticas**

Hora y lugar

1. Días: **Martes y Jueves**
2. Hora: **18:00 a 20:30**
3. Ubicación: **Online u Offline**

Información del instructor

1. Nombre: **Ing. Alberto Guzmán Capli Cabello**
2. Oficina: **Asistencia Virtual constante en la Plataforma**
3. Contacto: **acapli@pol.una.py**, 0981744530
4. Perfil profesional:

Magíster en Tecnología de la Información y Comunicación con Énfasis en Redes de Datos, Especialista en Ciberdefensa y Ciberseguridad Estratégica, Ingeniero en Informática, egresado de la Facultad Politécnica - UNA. Con cursos de Cisco Certified Network Associate (CCNA), Servidores Blade, Storage, SAN Switch, IPv6, IoT, entre otros, y 12 años de experiencia administrando Redes y Servidores, incluyendo la FPUNA y el Ministerio de Educación y Ciencias. Ex Director de Proyectos TIC en el Centro Nacional de Computación (CNC) de la UNA, ex Coordinador de Ciberseguridad de la Facultad Politécnica – UNA, y actualmente Especialista Técnico en Infraestructura del Ministerio de Tecnología de la Información y Comunicación, gestionando conectividades a nivel país. Con 9 años de experiencia como docente de Redes de Computadoras en la FP-UNA.

Notas adicionales

1. Se anima a los estudiantes a comunicarse con el instructor a través de los datos de contacto proporcionados para cualquier consulta o inquietud relacionada con el curso.
2. Es importante asistir tanto a las sesiones teóricas como a las prácticas para beneficiarse plenamente de la estructura del curso.

Prerrequisito

Ninguno.

Descripción del Curso

El curso de Seguridad de Redes y Nube está meticulosamente diseñado para abordar la necesidad crítica de experiencia en ciberseguridad en el panorama en rápida evolución de las redes digitales y la computación en la nube. Este curso ofrece una exploración integral de las teorías fundamentales y las estrategias prácticas necesarias para proteger los sistemas en red modernos y los servicios basados en la nube. Al profundizar en las complejidades de la seguridad de la red, los modelos de seguridad en la nube y las últimas tecnologías de ciberseguridad, los estudiantes están preparados para navegar y mitigar los complejos desafíos de seguridad que enfrentan las organizaciones actuales.

Un elemento central del curso es un análisis en profundidad de las técnicas criptográficas, los protocolos de seguridad y los principios que sustentan las arquitecturas de redes seguras. Los estudiantes abordarán temas como el cifrado, la autenticación y el diseño de políticas de seguridad, obteniendo una sólida comprensión de cómo se aplican estos elementos para proteger la información y garantizar la privacidad. El plan de estudios enfatiza el papel fundamental de la criptografía en la seguridad de las comunicaciones y los datos digitales, brindando a los estudiantes las habilidades para implementar estrategias de cifrado efectivas.

Al abordar los desafíos únicos de la computación en la nube, el curso cubre conceptos esenciales de seguridad en la nube, incluida la gestión de identidad y acceso (IAM), la protección de datos en la nube y el cumplimiento de los estándares regulatorios. Los estudiantes explorarán varios modelos de servicios en la nube (IaaS, PaaS, SaaS) y estrategias de implementación (pública, privada, híbrida), aprendiendo a diseñar y evaluar medidas de seguridad que se alineen con las necesidades específicas de los entornos basados en la nube. Este segmento garantiza que los graduados estén bien equipados para gestionar los requisitos de seguridad de los servicios en la nube, una habilidad cada vez más demandada en el campo de la ciberseguridad.

La experiencia práctica constituye la columna vertebral del enfoque de aprendizaje, con sesiones de laboratorio y ejercicios que simulan escenarios de seguridad del mundo real. Mediante el uso de herramientas y software de seguridad actuales, los estudiantes realizarán evaluaciones de vulnerabilidad, participarán en la detección y respuesta a amenazas y aplicarán políticas de seguridad en entornos prácticos. Este aprendizaje experiencial se complementa con un proyecto final que desafía a los estudiantes a diseñar, implementar y

evaluar el marco de seguridad para una red o sistema en la nube, integrando los conocimientos y habilidades adquiridos a lo largo del curso.

El curso no solo prepara a los estudiantes para roles técnicos en ciberseguridad, sino que también cultiva una comprensión de las implicaciones éticas y legales de las prácticas de seguridad digital. Los debates sobre piratería ética, privacidad de datos y cumplimiento de las normas legales garantizan que los graduados no sólo sean técnicamente competentes sino también administradores responsables de la seguridad de la información. Al final del curso, los estudiantes tendrán una comprensión integral de la seguridad de la red y la nube, equipados con el conocimiento teórico y las habilidades prácticas para sobresalir en el dominio de la ciberseguridad.

Características clave:

- **Marco teórico en profundidad:** los estudiantes obtendrán una comprensión sólida de los fundamentos teóricos de la seguridad de las redes y la nube. Esto incluye una exploración de protocolos criptográficos, modelos de seguridad y los principios del diseño de redes seguras. Se hará hincapié en comprender el "por qué" detrás de las medidas de seguridad, lo que permitirá a los estudiantes adaptarse al panorama de amenazas en constante evolución.
- **Prácticas de seguridad en la nube de vanguardia:** el curso proporciona un examen exhaustivo de la seguridad en la nube, centrándose en las últimas prácticas, herramientas y tecnologías. Se cubrirán temas como la protección de datos en la nube, la arquitectura segura de la nube y los estándares de cumplimiento de la nube (por ejemplo, FedRAMP, GDPR). Los estudiantes aprenderán a afrontar los desafíos de seguridad únicos que presenta la computación en la nube, desde problemas de múltiples inquilinos hasta vulnerabilidades específicas de la nube.
- **Experiencia de aprendizaje práctico:** reconociendo la importancia de las habilidades prácticas, el curso incluye sesiones de laboratorio y ejercicios prácticos que simulan escenarios del mundo real. Los estudiantes interactuarán con herramientas y plataformas de seguridad contemporáneas, realizarán evaluaciones de vulnerabilidad e implementarán medidas de seguridad en un entorno controlado. Este enfoque práctico garantiza que los estudiantes no sólo tengan conocimientos sino que también sean capaces de aplicar sus habilidades en entornos del mundo real.
- **Enfoque en tecnologías emergentes:** el plan de estudios tiene visión de futuro eincorpora debates sobre las implicaciones de seguridad de las tecnologías emergentes como Internet de las cosas (IoT), inteligencia artificial (IA) en ciberseguridad y blockchain. Esto prepara a los estudiantes para futuros desafíos y oportunidades en seguridad de redes y nubes.
- **Aprendizaje basado en proyectos:** un componente importante del curso es un proyecto final que requiere que los estudiantes apliquen su aprendizaje para diseñar y evaluar la seguridad de una red o infraestructura de nube. Este proyecto fomenta el pensamiento crítico, la resolución de problemas y las habilidades de gestión de proyectos, preparando a los estudiantes para roles profesionales en el campo de la ciberseguridad.
- **Entorno de aprendizaje colaborativo:** el curso fomenta la colaboración a través de proyectos grupales, revisiones de pares y foros de discusión. Este enfoque colaborativo mejora los resultados del aprendizaje y prepara a los estudiantes para la naturaleza orientada al trabajo en equipo del trabajo de ciberseguridad.

- **Contenido relevante para la industria:** el plan de estudios está diseñado con aportes de profesionales de la industria, lo que garantiza que el contenido sea relevante y esté actualizado con los estándares y prácticas actuales. Las conferencias invitadas de expertos en el campo brindarán información sobre los desafíos y expectativas de las funciones de ciberseguridad.
- **Consideraciones éticas y legales:** la piratería ética, las consideraciones de privacidad y el cumplimiento de los estándares legales son partes integrales del curso. Los estudiantes aprenderán la importancia de la conducta ética en las prácticas de ciberseguridad y las implicaciones legales de las medidas de seguridad.

Este curso no se trata solo de aprender a proteger los activos digitales; se trata de comprender el panorama de las amenazas y oportunidades de la ciberseguridad, dominar las herramientas y técnicas para mitigar los riesgos y prepararse para el futuro de la seguridad de las redes y la nube. A través de una combinación de conocimientos teóricos y habilidades prácticas, los estudiantes saldrán de este curso listos para contribuir de manera efectiva al campo de la ciberseguridad.

Objetivo del Curso

Al completar con éxito este curso, los estudiantes podrán:

1. Comprender los conceptos fundamentales de seguridad de redes y computación en la nube.
2. Identificar y evaluar riesgos de seguridad en entornos de red y nube.
3. Implementar medidas de seguridad para proteger datos, aplicaciones e infraestructuras.
4. Aplicar tecnologías de cifrado y mecanismos de control de acceso.
5. Diseñar y evaluar políticas y procedimientos de seguridad.
6. Utilizar herramientas y software de seguridad para la detección y análisis de amenazas.
7. Comprender las cuestiones legales, éticas y de cumplimiento relacionadas con la seguridad de la red y la nube.

- **Comprender los conceptos fundamentales de seguridad de redes y computación en la nube:**
    - Obtener una comprensión integral de la arquitectura, los componentes y las operaciones de las redes y las plataformas de computación en la nube.
    - Explorar la evolución de la seguridad de la red y la computación en la nube, comprendiendo su importancia en el panorama digital actual.
- **Identificar y evaluar riesgos de seguridad en entornos de red y nube:**
    - Aprender a identificar de forma proactiva posibles vulnerabilidades y amenazas de seguridad tanto en configuraciones de red tradicionales como en entornos de nube.
    - Desarrollar la capacidad de realizar evaluaciones de riesgos, entendiendo la probabilidad y el impacto de los riesgos de seguridad identificados.
- **Implementar medidas de seguridad para proteger datos, aplicaciones e infraestructuras:**

    - Adquirir experiencia práctica en la implementación de soluciones de seguridad que protejan los activos digitales contra accesos no autorizados, filtraciones de datos y otras amenazas cibernéticas.
    - Comprender la implementación de firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), así como medidas de seguridad específicas de los servicios en la nube, como el cifrado de datos en reposo y en tránsito.
- **Aplicar tecnologías de cifrado y mecanismos de control de acceso:**
    - Dominar los principios de los algoritmos criptográficos, la gestión de claves y las firmas digitales para garantizar la confidencialidad, integridad y autenticidad de la información.
    - Implementar estrategias de control de acceso, incluido el control de acceso basado en roles (RBAC), para garantizar que solo los usuarios autorizados puedan acceder a recursos específicos.
- **Diseñar y evaluar políticas y procedimientos de seguridad:**
    - Desarrollar las habilidades para crear políticas de seguridad integrales que gobiernen la protección de los activos de información, abordando áreas como el uso aceptable, la clasificación de datos y la respuesta a incidentes.
    - Aprender a evaluar y actualizar políticas y procedimientos de seguridad para adaptarse a nuevas amenazas y requisitos de cumplimiento.
- **Utilizar herramientas y software de seguridad para la detección y análisis de amenazas:**
    - Adquirir competencia en el uso de herramientas y software de seguridad contemporáneos para monitorear, detectar y analizar incidentes de seguridad.
    - Participar en laboratorios prácticos y simulaciones para practicar la respuesta a incidentes, la búsqueda de amenazas y el uso de sistemas de gestión de eventos e información de seguridad (SIEM).
- **Comprender las cuestiones legales, éticas y de cumplimiento relacionadas con la seguridad de la red y la nube:**
    - Examinar los marcos legales y las consideraciones éticas que rodean la seguridad de la red y la nube, incluida las leyes de protección de datos, los estándares de cumplimiento normativo y la piratería ética.
    - Prepararse para navegar las complejidades de las auditorías de cumplimiento y garantizar que las prácticas de seguridad cumplan con los estándares legales y éticos.

Al lograr estos objetivos, los estudiantes estarán bien preparados para ingresar al campo de la ciberseguridad con una base sólida en los principios de seguridad de la red y la nube.
Poseerán el pensamiento crítico y las habilidades de resolución de problemas necesarios para abordar los desafíos de seguridad del mundo real, lo que los convertirá en activos valiosos para cualquier organización que busque mejorar su postura de ciberseguridad.

Política de Calificación

La calificación del curso se estructura de la siguiente manera para evaluar la comprensión, el compromiso y la aplicación práctica del material del curso por parte de los estudiantes:

1. Asistencia: 20% de la nota final. La asistencia regular es crucial ya que refleja el compromiso y la participación del estudiante en el proceso de aprendizaje.
2. Tareas y Pruebas: 50% de la nota final. Este componente integral evalúa la comprensión de los estudiantes del material del curso a través de tareas y pruebas regulares. Estas tareas están diseñadas para reforzar el aprendizaje y garantizar un compromiso continuo con el contenido del curso.
3. Examen Parcial: 15% de la nota final. El examen de mitad de período evalúa la comprensión de los estudiantes de los conceptos y principios clave cubiertos en la primera mitad del curso.
4. Examen Final: 15% de la nota final. El examen final se centra en todo el contenido del curso, poniendo a prueba la comprensión general de los estudiantes y su capacidad para integrar diferentes temas aprendidos a lo largo del curso.

Esta política de calificación está diseñada para evaluar de manera justa el desempeño de los estudiantes en diferentes aspectos del curso, fomentando el esfuerzo constante, la participación activa y una comprensión profunda de la materia.

Tareas y Exámenes

Para garantizar una evaluación integral de la comprensión y aplicación de los conceptos de seguridad de red y nube de los estudiantes, el curso incorporará una combinación de tareas, exámenes y un proyecto final. Cada componente de evaluación está diseñado para evaluar diferentes facetas de los conocimientos y habilidades de los estudiantes, garantizando que estén bien preparados para los desafíos de ciberseguridad del mundo real.

Tareas

- Tareas prácticas: estas tareas prácticas requerirán que los estudiantes utilicen herramientas y software de seguridad para tareas como configurar firewalls, realizar análisis de vulnerabilidades e implementar cifrado. El objetivo es reforzar los conocimientos teóricos a través de la aplicación práctica, permitiendo a los estudiantes adquirir experiencia con las herramientas y técnicas utilizadas en el campo.
- Estudios de casos: los estudiantes analizarán incidentes de ciberseguridad del mundo real, centrándose en las vulnerabilidades explotadas, el impacto en las organizaciones involucradas y las medidas tomadas en respuesta. Esto desarrollará su capacidad para evaluar y responder a las amenazas a la seguridad.
- Artículos de investigación: las tareas también pueden incluir la redacción de artículos de investigación sobre tecnologías, tendencias y/o desafíos emergentes de seguridad de redes y nubes. Esto alentará a los estudiantes a involucrarse con el estado actual de la investigación en ciberseguridad y a considerar direcciones futuras para el campo.

Exámenes

- Examen parcial: evaluará la comprensión de los estudiantes de conceptos fundamentales en seguridad de redes y nubes, incluida la criptografía, los protocolos de seguridad y los principios básicos de seguridad de la computación en la nube. Constará de preguntas de opción múltiple, respuestas cortas y escenarios de resolución de problemas.
- Examen final: será integral y cubrirá todo el contenido del curso con un enfoque en la aplicación de medidas de seguridad, evaluación de riesgos y el diseño de políticas y procedimientos de seguridad. Incluirá una combinación de preguntas de opción múltiple, ensayos y análisis de estudios de casos para evaluar el dominio de los estudiantes del material del curso.

Proyecto Final

- Objetivo del proyecto: El proyecto final requerirá que los estudiantes diseñen e implementen una solución de seguridad para una red hipotética o un entorno de nube. Este proyecto abarcará la evaluación de riesgos, la aplicación de medidas de seguridad y el desarrollo de políticas y procedimientos de seguridad.
- Fases del proyecto: El proyecto se dividirá en varias fases, que incluyen planificación, diseño, implementación y evaluación. Se espera que los estudiantes realicen lo siguiente.
    - Planificar: Identificar los requisitos y objetivos de seguridad para el entorno seleccionado.
    - Diseñar: Desarrollar una arquitectura de seguridad que aborde los riesgos identificados y cumpla con los requisitos definidos.
    - Implementar: Aplicar medidas y controles de seguridad para proteger el medio ambiente.
    - Evaluar: Evaluar la efectividad de la solución de seguridad y presentar recomendaciones de mejora.
- Presentación: Los estudiantes presentarán sus proyectos a la clase, demostrarán su solución de seguridad y discutirán el fundamento detrás de sus elecciones de diseño. Esto fomentará el aprendizaje entre pares y brindará la oportunidad de recibir comentarios constructivos

Este enfoque estructurado de las tareas, los exámenes y el proyecto final garantiza que los estudiantes no sólo comprendan los conceptos teóricos sino que también adquieran experiencia práctica y habilidades en el monitoreo y evaluación de redes. El énfasis en la aplicación, el análisis y la comunicación prepara a los estudiantes para los desafíos del mundo real en la gestión de redes y los posiciona para el éxito en sus futuras carreras.

Actividad del Curso

Para enriquecer la experiencia de aprendizaje y garantizar una comprensión profunda de la seguridad de red y nube, el curso incorporará una variedad de actividades diseñadas para atender diferentes estilos y preferencias de aprendizaje. Estas actividades están estructuradas para promover el compromiso, facilitar el aprendizaje práctico y fomentar la aplicación de conceptos teóricos en escenarios del mundo real.

Charlas y Debates

- Charlas interactivas: las clases del curso incluirán elementos interactivos como encuestas en tiempo real, sesiones de preguntas y respuestas y debates sobre tendencias y noticias actuales en ciberseguridad. Este enfoque fomenta la participación activa y mantiene a los estudiantes interesados con el material.
- Oradores invitados: invitar a profesionales y expertos de la industria como oradores invitados proporcionará información valiosa sobre los aspectos prácticos de la seguridad de la red y la nube, asesoramiento profesional y las últimas tendencias de la industria.

Sesiones de Laboratorio

- Laboratorios prácticos: las sesiones de laboratorio dedicadas permitirán a los estudiantes trabajar con herramientas y tecnologías de seguridad en un entorno controlado. Estas sesiones incluirán actividades como instalar y configurar medidas de seguridad, realizar pruebas de penetración e implementar configuraciones seguras en la nube.
- Ejercicios de simulación: se utilizarán incidentes de ciberseguridad simulados para enseñar a los estudiantes cómo responder a las violaciones de seguridad. Estos ejercicios ayudarán a desarrollar el pensamiento crítico y la capacidad de tomar decisiones bajo presión.

Trabajos y Colaboraciones Grupales

- Proyectos en equipo: los estudiantes se agruparán para trabajar en proyectos más pequeños a lo largo del curso, como diseñar una arquitectura de red segura o desarrollar una política de seguridad en la nube para una organización hipotética. El trabajo en equipo fomenta la colaboración y permite a los estudiantes aprender de las fortalezas y perspectivas de los demás.
- Revisión por pares: las tareas y proyectos pueden incluir un componente de revisión por pares, donde los estudiantes brindan retroalimentación sobre el trabajo de los demás. Esto fomenta un entorno de aprendizaje colaborativo y ayuda a los estudiantes a perfeccionar sus habilidades de evaluación críticas.

Foros y Debates en Línea

- Foros de discusión: se utilizarán foros en línea para discusiones fuera del horario de clase, lo que permitirá a los estudiantes publicar preguntas, compartir recursos y participar en discusiones sobre diversos temas relacionados con el curso. Esto facilita el aprendizaje continuo y la interacción entre estudiantes e instructores.
- Discusiones de estudios de casos: se pueden dedicar foros específicos a discutir estudios de casos, donde los estudiantes pueden analizar y debatir el manejo de

incidentes de ciberseguridad del mundo real, mejorando sus habilidades analíticas y su comprensión de la ciberseguridad en la práctica.

Pruebas y Auto-evaluación

- Pruebas semanales: cuestionarios semanales breves ayudarán a reforzar los conceptos cubiertos en las conferencias y lecturas, proporcionando retroalimentación inmediata a los estudiantes sobre su comprensión del material.
- Ejercicios de autoevaluación: estos ejercicios permitirán a los estudiantes evaluar su propio progreso y comprensión del material del curso, identificando áreas en las que pueden necesitar centrar más atención.

Talleres y Seminarios

- Talleres de ciberseguridad: los talleres especializados que se centran en herramientas, técnicas o temas específicos (por ejemplo, piratería ética, análisis forense digital) proporcionarán inmersiones profundas en áreas de particular interés o importancia.
- Seminarios sobre cuestiones éticas y legales: los seminarios dedicados cubrirán los aspectos éticos y legales de la ciberseguridad, incluidas discusiones sobre leyes de privacidad, requisitos de cumplimiento y la ética de la piratería. Estas sesiones ayudarán a los estudiantes a navegar por el complejo panorama moral y legal de la ciberseguridad.

Estas variadas actividades del curso están diseñadas para crear un entorno de aprendizaje dinámico e interactivo, que atiende las diversas necesidades e intereses de los estudiantes y al mismo tiempo los equipa con los conocimientos y habilidades necesarios para carreras en seguridad de redes y nube.

Cronograma del Curso

1. Fundamentos de la computación en la nube
2. Seguridad en Infraestructura de Redes
3. Seguridad en Sistemas Operativos Linux
4. Amenazas y vulnerabilidades
5. Medidas de protección
6. Seguridad en la nube
7. Respuesta a Incidentes y Recuperación
8. Políticas de seguridad y cumplimiento
9. Firewalls: Filtros, Proxy, NAT

Semana	Clase
1	Fundamentos de la computación en la nube
2	Seguridad en Infraestructura de Redes Seguridad en Sistemas Operativos Linux
3	Amenazas y vulnerabilidades Medidas de protección
4	Examen Parcial / Proyecto
5	Seguridad en la nube
6	Políticas de seguridad y cumplimiento
7	Firewalls: Filtros, Proxy, NAT
8	Examen Final / Proyecto