Fecha: diciembre de 2021

PROGRAMA ACADÉMICO: Ingeniería de Sistemas y Computación

SEMESTRE: Décimo

ASIGNATURA: Electiva III - Gestión de la seguridad de la infraestructura telemática

CÓDIGO: 8108281

NÚMERO DE CRÉDITOS: 3

PRESENTACIÓN

Para el curso de gestión de la seguridad de la infraestructura telemática se fundamenta en el ciclo de telecomunicaciones, accederá a tener un análisis inicial de las características principales de la infraestructura de una organización desde las pequeñas empresas a unos niveles elevados de complejidad de infraestructura telemática y sus posibles puntos de debilidad para tomar medidas de corrección apoyados en los conceptos previamente vistos.

Se debe enfatizar que para el desarrollo de esta asignatura complementara la línea formativa de redes telemáticas, redes de datos que integraría a la fundamentación, profundización e investigación de esta.

JUSTIFICACIÓN

El mundo está girando entorno a niveles de información digital incremental y mucha de esta información digital es sensible para las compañías que trabajan arduamente por mantener a salvo y confiablemente su información digital para su crecimiento económico, por lo tanto, manteniendo que la seguridad de su información sea correcta al momento de ser divulgada, sin embargo, existen excepciones a la regla y ataques inesperados, los cuales conllevan a perdidas de baja escala o a perdidas de grandes dimensiones en las compañías. Partiendo de la pregunta para la materia ¿Es mi organización segura? Se mostrará un panorama diferente de la normalidad en que se utilizan los canales de comunicación de la infraestructura telemática, la gestión de la seguridad infraestructura telemática y el cómo existe una posibilidad de ser vulnerados sin darnos cuenta de las consecuencias incrementales y los niveles que puede llegar a tener un usuario mal intencionado.

Para mitigar las consecuencias se debe llegar a entender cómo se gestiona la seguridad de la infraestructura telemática y las consecuencias tanto para la empresa, como la parte legal y llevar a cabo un plan de desarrollo de cadena de trabajo para mantener el Core central de la compañías en las óptimas condiciones posibles entendiendo que nada es 100% seguro, sin embargo tenemos un porcentaje de 99% de buscar estar seguros, gestionando los escenarios, basándonos y apoyándonos en los conocimientos de la línea de comunicaciones, transmisión de datos, redes y telemática.

Los futuros profesionales estarán proyectados a el correcto funcionamiento de la línea telemática, adicionalmente tendrán la parte de gestión de la seguridad de la infraestructura telemática para mitigación de incidentes, además estarán delante de las posibles consecuencias para las compañías llegando a mejorar y ampliar sus conocimientos en la disciplina para su proyección profesional.

COMPETENCIAS

Se busca dentro de la asignatura promover el desarrollo de competencias:

- Competencia Ética profesional.
- Competencia Comunicativa.
- Competencia Crítica y creativa.
- Competencia Analítica.
- Competencia Experimental.
- Competencia Tecnológica.

Dando lugar al final de la materia que el estudiante:

- Identifica el proceso de gestión de redes de la compañía con el enfoque mitigativo del riesgo inherente.
- Analizar las posibles causas de la vulneración.
- Identifica las características de un modelo de referencia general de infraestructura.
- Identifica las características técnicas y funcionales para la gestión de la seguridad de la infraestructura telemática.
- Caracteriza los distintos medios de intrusión.
- Construye técnicamente interfaces de red.
- Identifica las normas de estándar de seguridad.
- Compara los métodos para la detección de seguridad e inseguridad.

RESULTADOS DE APRENDIZAJE

- Identifico el proceso de gestión de redes de la compañía con el enfoque mitigativo del riesgo, orientadas a asegurar la integridad de la información de la organización.
- Reconozco las características técnicas y funcionales para la gestión de la seguridad de la infraestructura telemática, y los distintos medios de intrusión, acorde a las normas y estándares de seguridad, y de esta manera evaluar los riesgos y su mitigación.
- Resuelvo casos de estudio reales y prácticos, relacionados con la características técnicas y funcionales de la gestión de la seguridad de la infraestructura telemática, demostrando gran capacidad de análisis, síntesis, trabajo en equipo e Investigación, tanto a nivel académico como profesional.

METODOLOGÍA

Esta asignatura será guiada en los espacios presenciales por la complementación conceptual del docente al trabajo de preparación previo que los estudiantes han realizado sobre la temática particular a tratar en la sesión; por lo tanto, un tema será abarcado en cinco momentos:

1. Preparación, consulta e investigación conceptual por cuenta del estudiante y su pequeño grupo de trabajo.
2. Tratamiento conceptual del tema en sesión del gran grupo junto con el docente.
3. Aplicación de talleres individuales y cooperativos a nivel tutorial.
4. Desarrollo de actividades de refuerzo en sesiones autónomas.
5. Practica en laboratorio para ejercer los conceptos puestos en clase.

De lo anterior se verifica que en la actividad 1, el estudiante constituirá conflictos conceptuales de baja complejidad, a solucionar en el transcurso de la actividad 2, entre tanto, la actividad 4 generará conflictos

cognitivos orientados a la aplicación, a subsanar con la actividad 3, en la actividad 5 se busca solventar el conflicto imaginario y real en la práctica de laboratorio.

Se considera que el estudiante debe alcanzar un amplio trabajo autónomo, que posteriormente será complementado por el trabajo cooperativo de su pequeño grupo.

La generación de conflictos cognitivos es importante y necesaria, para que las sesiones de gran grupo cumplan con su objetivo de afianzamiento del conocimiento.

INVESTIGACIÓN

La asignatura de manera intrínseca permite la investigación formativa durante la exploración de cada una de las temáticas asociadas. A su vez, dentro de la metodología, los estudiantes deberán explorar diferentes recursos de literatura científica y técnica que garanticen la comprensión del estado de avance y tendencias en los temas propios de la asignatura.

El avance en las prácticas de asignatura y proyecto final promueven el apoyo por parte del grupo de estudio en Gestión de la Seguridad de la Infraestructura Telemática que existe en el programa de Ingeniería de Sistemas y Computación.

MEDIOS AUDIOVISUALES

Video Beam, recurso computacional, equipos de comunicaciones, según disposición institucional.

EVALUACIÓN

EVALUACIÓN COLECTIVA

La evaluación tiene un carácter formativo donde es imprescindible el reconocimiento del error como punto de partida para la mejora, incremento y refinamiento de capacidades.

A nivel conceptual se posibilita la aplicación de exámenes y talleres a nivel individual y grupal.

El aporte del estudiante correrá por cuenta de la preparación conceptual individual de los temas previamente a cada sesión, su complemento al trabajo en grupal, la transferencia del conocimiento, la presentación de exposiciones y la demostración de sus capacidades de análisis, síntesis y redacción, plasmadas en ensayos y artículos bajo estrictos criterios de publicación científica.

Didácticamente se aprovecharán los elementos que brindan la auto, co y hetero-evaluación.

La asignatura promueve la asociación de estudiantes para cumplir con objetivos comunes, a través de grupos de trabajo.

EVALUACIÓN INDIVIDUAL

El cálculo de la nota final se hará de la siguiente manera:

Nota Única 100%
20% Parcial
20% Quices y Trabajos

15% Exposición
20% Talleres- Prácticas
5% Auto-evaluación y Hetero-evaluación
20%Proyecto Final

CONTENIDOS TEMÁTICOS CENTRALES

1. Introducción – Policía Marco Legal
2. Infraestructura de red.
3. Arquitectura general de infraestructura.
4. Delineación de la seguridad básica.
5. Bases de datos y la infraestructura telemática.
6. Administración Segura.
7. Commerce Server
8. Servidores de seguridad
9. Proceso de prueba - Estándares
10. Diagrama completo del sistema y proyecto final

LECTURAS MÍNIMAS

Artículos y apartados bibliográficos de los diferentes temas a tratar, proporcionados por el Docente. Consulta permanente a los foros de las organizaciones, empresas productoras de tecnología y estándares en Seguridad Informática.

BIBLIOGRAFÍA

- Infraestructuras comunes de telecomunicaciones y radiocomunicaciones. Perales Benito, Tomás. Alfaomega. 2014
- Redes y Comunicación de datos en los negocios. Fitzgerald, Dennis. Noriega Limusa. Tercera edición. México. 2003
- Transmisión de datos y redes de comunicaciones. Behrouz A. Forouzan. Segunda edición Mc Graw Hill. Madrid 2002
- Transmisión de datos y Redes de Computadores. García Teodoro, Pedro; Díaz Verdejo Jesús Esteban; López soler, Juan Manuel. Pearson Educación, S.A. Madrid 2003
- Redes de computadores. Andrew S. Tenenbaum. Prentice Hall.Cuarta Edución. 2003
- Comunicaciones y redes de computadores. William Stallings. Séptima Edición. Prentice Hall