

Actividad de Aprendizaje

NOMBRE DEL MÓDULO

Configuración de la seguridad en redes de área local.

NOMBRE DE LA ACTIVIDAD DE APRENDIZAJE

Verificar algoritmos de seguridad.

APRENDIZAJES ESPERADOS

5.4 Evalúa la seguridad de una red utilizando técnicas de criptografía, reconocimiento, escaneo, proponiendo recomendaciones en un informe de hallazgos y brechas de seguridad encontrados.

CRITERIOS DE EVALUACIÓN

5.4.2 Recopila información de los distintos sistemas informáticos de una red de área local.

5.4.3 Analiza una aplicación, sistema o red en busca de una posible vulnerabilidad.

5.4.4 Genera un informe con toda la información recolectada y propone recomendaciones de seguridad a la red de área local.

OBJETIVOS DE APRENDIZAJE GENÉRICOS

A - Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.

- C** - Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas
- D** - Trabajar eficazmente en equipo, coordinando acciones con otros, in situ o a distancia, solicitando y prestando cooperación para el buencumplimiento de sus tareas habituales o emergentes.
- H** - Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.

METODOLOGÍA SELECCIONADA

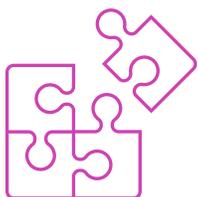
Simulación en contextos laborales.

Competencias Desagregadas



CONOCIMIENTOS

- ▶ Conocimiento de conceptos básicos de ciberseguridad.
- ▶ Conocimiento de estándares y procedimientos de ciberseguridad.
- ▶ Análisis e interpretación de datos relacionados con vulnerabilidades.
- ▶ Conocimiento de leyes y normativas chilenas relativas a ciberseguridad.



HABILIDADES

- ▶ Recopilación de información de un sistema informático.
- ▶ Enumeración como escaneo de puertos.
- ▶ Recolección de datos en búsqueda de vulnerabilidad.
- ▶ Comunicación oral y por escrito con claridad.
- ▶ Manejo de tecnología de información y comunicación.



ACTITUDES

- ▶ Cooperación de manera eficaz, prolija y rigurosa en el trabajo en equipo.
- ▶ Cumplimiento en la entrega de trabajos dentro de plazos establecidos.

Descripción de Tareas y Recursos



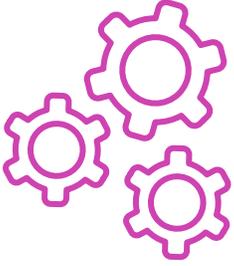
PREPARACIÓN DE LA ACTIVIDAD

Docente

- ▶ Revisa todos los recursos de la actividad y, en caso de ser necesario, realiza las adecuaciones correspondientes, para estimular la generación de un ambiente de aprendizaje donde los y las estudiantes construyan colaborativamente una experiencia significativa y enriquecedora para su proceso de desarrollo personal y social.
- ▶ En caso de ser necesario, imprime materiales para el desarrollo de la actividad.

Recursos:

- ▶ Presentación en **PPT “Recomendaciones de Ciberseguridad en base a detección y análisis de vulnerabilidades”**.
- ▶ Actividad de Aprendizaje **“Test de seguridad e informe técnico”**.
- ▶ Actividad de Evaluación (Material para docente) y su instrumento de evaluación (rúbrica y lista de cotejo).
- ▶ Actividad de Evaluación **“Informe técnico: evidencias de vulneración y recomendaciones”**.
- ▶ Ticket de salida **“Test de seguridad e informe técnico de vulnerabilidades”**.
- ▶ Infografía **“Ciclo de auditoría de seguridad ofensiva”**.
- ▶ Video de metodología **“Simulación en contextos laborales”**.
- ▶ Revisar Presentación **“Recursos compartidos a través de una red de área local: vulnerabilidades, matriz de riesgo y plan de acción”**.



EJECUCIÓN

Docente:

- ▶ Promueve una atmósfera de respeto mutuo y empatía con la diversidad durante toda la clase.
- ▶ Comparte el Aprendizaje Esperado, los Criterios de Evaluación, los Objetivos de Aprendizaje de la Especialidad y los Objetivos de Aprendizaje Genéricos correspondientes, que se encuentran al inicio de la presentación **PPT “Recomendaciones de Ciberseguridad en base a detección y análisis de vulnerabilidades”**, así como la metodología que va a usar a partir del video **“Simulación en contextos laborales”**.
- ▶ Realiza un diagnóstico de conocimientos previos con preguntas al inicio de la clase.
- ▶ Explica la temática del PPT **“Recomendaciones de Ciberseguridad en base a detección y análisis de vulnerabilidades”**, respondiendo dudas e inquietudes que aparezcan en el proceso. Expone el contenido de la presentación contextualizando el aprendizaje con ejemplos vinculados al quehacer de la vida cotidiana y/o laboral.
- ▶ Indica la formación de equipos de trabajo de 2 estudiantes para la ejecución de la actividad de aprendizaje.
- ▶ Entrega las instrucciones para la ejecución de la Actividad de Aprendizaje **“Test de seguridad e informe técnico”**.
- ▶ El o la docente da retroalimentación y responde dudas de los y las estudiantes.
- ▶ Realiza la Actividad de evaluación **“Informe técnico: evidencias de vulneración y recomendaciones”** y verifica que los aspectos claves del trabajo se cumplan mediante la **lista de cotejo**.

Estudiantes:

- ▶ Participan en la construcción colaborativa de una experiencia significativa y enriquecedora de su proceso de desarrollo personal y social, coadyuvando a una atmósfera de respeto mutuo y empatía con la diversidad.
- ▶ Escuchan con atención el Aprendizaje Esperado, los Criterios de Evaluación, los Objetivos de Aprendizaje de la Especialidad y los Objetivos de Aprendizaje Genéricos correspondientes, así como la metodología con la que van a usar.
- ▶ Participan en las preguntas de diagnóstico de conocimientos previos y ayudan a la contextualización del aprendizaje proponiendo ejemplos vinculados al quehacer de la vida cotidiana y/o laboral.
- ▶ Escuchan con atención la presentación de PPT “Recomendaciones de Ciberseguridad en base a detección y análisis de vulnerabilidades”, e interactúan durante ésta para resolver sus dudas.
- ▶ Forman los equipos de trabajo para participar en la Actividad de Aprendizaje “Test de seguridad e informe técnico”.
- ▶ Preguntan sus dudas durante la actividad y reciben la infografía “Ciclo de auditoría de seguridad ofensiva” como material de apoyo.
- ▶ Realizan la Actividad de evaluación “Informe técnico: evidencias de vulneración y recomendaciones”.
- ▶ Son evaluados mediante rúbricas de evaluación y pautas de cotejo pertinentes.



CIERRE

Docente:

- ▶ Entrega retroalimentación de las correcciones efectuadas con la Pauta de Cotejo a la Actividad de evaluación “**Informe técnico: evidencias de vulneración y recomendaciones**”.
- ▶ Genera el cierre de la actividad, realizando un plenario con las impresiones y preguntas hacia y desde las y los estudiantes, incentivando las respuestas del **Ticket de salida “Test de seguridad e informe técnico de vulnerabilidades”**.

Estudiantes:

- ▶ Participan del plenario compartiendo sus impresiones de la actividad de y respondiendo las preguntas generadas por el o la docente provenientes del Ticket de salida “**Test de seguridad e informe técnico de vulnerabilidades**” y las que surjan de ellos. A su vez, reflexionan sobre su competencia genérica de trabajo en equipo (fortalezas, debilidades, aspectos a mejorar).

Información complementaria



EQUIPAMIENTO Y MOBILIARIO (DECRETO 240)

PC escritorio o Portátil.

Packet Tracer (Simulación de Laboratorio).

Router o Switch (Laboratorio).

Cable Consola (Laboratorio).

Software Putty (Laboratorio).

Proyector.

Otros: Documento Protocolos de acceso remoto (recomendado).

ESTRATEGIA DE ALTERNANCIA

Pasantías en empresas del sector productivo, servicios y/o empresas públicas, retail, oficinas contables y otras.

