CONSEJO NACIONAL DE RECTORES

Oficina de Planificación de la Educación Superior

División Académica

DICTAMEN SOBRE LA REVISIÓN CURRICULAR DEL PROGRAMA DE TÉCNICO 3 EN CIBERSEGURIDAD DE LA UNIVERSIDAD NACIONAL

Alexander Cox Alvarado

OPES; no. 09-2024

378.2
C877d

Cox Alvarado, Alexander.
Dictamen sobre la revisión curricular del programa de técnico 3 en ciberseguridad de la Universidad Nacional. [Recurso electrónico] / Alexander Cox Alvarado – Datos electrónicos (1 archivo : 400 kb). -- San José, C.R. : CONARE - OPES, 2024.
(OPES; no. 09-2024)

ISBN 978-9977-77-592-0
Formato pdf, (47 páginas.)

1. REVISIÓN CURRICULAR. 2. CIBERSEGURIDAD. 3. TÉCNICO UNIVERSITARIO. 4. PERFIL PROFESIONAL. 5. PLAN DE ESTUDIOS. 6. PERSONAL DOCENTE. 7. UNIVERSIDAD NACIONAL (COSTA RICA). I. Título. II. Serie.

LRD

PRESENTACIÓN

El análisis que se presenta en este documento (OPES; no. 09-2024) se refiere al dictamen sobre la revisión curricular del Programa de Técnico 3 en Ciberseguridad de la Universidad Nacional.

El dictamen fue realizado por el M.Sc. Alexander Cox Alvarado, investigador de la División Académica de la Oficina de Planificación de la Educación Superior (OPES) con base en documentos enviados por la Universidad Nacional.

La revisión del documento estuvo a cargo de la Dra. Katalina Perera Hernández, Jefa de la División Académica y la edición del documento fue realizada por Sandra Guillén Guardado, asistente de la División citada.



Katalina Perera Hernández
Jefa División Académica
OPES, Conare

Tabla de contenido

1. Introducción 1
2. Datos generales 2
3. Objeto de estudio 2
4. Propósitos 2
5. Requisitos de ingreso 3
6. Justificación 3
7. Alineación de la propuesta curricular con el estándar de cualificación 4
8. Cumplimiento de horas de la propuesta curricular en relación con el nivel de técnico estipulado por el MNC-EFTP-CR 4
9. Correspondencia de las competencias con el estándar de cualificación 4
10. Estrategias metodológicas de mediación 10
11. Correspondencia del equipo docente con las actividades académicas 11
12. Conclusiones 11
13. Anexos 13

ANEXO A Estructura curricular 13
ANEXO B Descripción de los módulos 15
ANEXO C Perfil del docente 47

1. Introducción

La solicitud de autorización del programa de Técnico 3 en Ciberseguridad fue enviada al Consejo Nacional de Rectores (CONARE) por el vicerrector de Docencia de la Universidad Nacional (UNA), M. Sc. Randall Hidalgo Mora, mediante el oficio UNA-VD-OFIC-120-2024 del 1 de febrero de 2024, con el objetivo de iniciar los procedimientos establecidos en el documento *Lineamientos para la revisión curricular por parte de OPES de los programas de Educación y Formación Técnica Profesional en las universidades estatales*[1]. Posteriormente, se recibió en CONARE el oficio UNA-VD-OFIC-88-2024 del 28 de junio de 2024 que subsanó una característica del programa presentado para que se alineara al *Marco Nacional de Cualificaciones de la Educación y Formación Técnica Profesional de Costa Rica* (MNC-EFTP-CR).

Cuando se solicita la autorización de un programa de técnico al CONARE, se utiliza lo establecido en los Lineamientos mencionados, los cuales señalan los siguientes temas, que serán la base del estudio realizado por la Oficina de Planificación de la Educación Superior (OPES) para autorizar el programa propuesto:

- Datos generales
- Objeto de estudio
- Propósitos
- Requisitos de ingreso
- Justificación.
- Alineación de la propuesta curricular con el estándar de cualificación.
- Cumplimiento de horas de la propuesta curricular en relación con el nivel de técnico estipulado por el MNC-EFTP-CR.
- Correspondencia de la competencia general con el estándar de cualificación, y entre las competencias específicas y resultados de aprendizaje en los contenidos o áreas temáticas de los cursos, módulos o bloques del técnico correspondientes al nivel técnico establecido en el MNC-EFTP-CR.

- Estrategias de mediación.
- Correspondencia del equipo docente con las actividades académicas.

A continuación, se analizará cada uno de estos aspectos.

[1] Aprobado por el Consejo Nacional de Rectores en su sesión 29-2020, celebrada el 21 de julio de 2020, mediante el acuerdo CNR-251-2020.

2. Datos generales

La unidad académica proponente del programa es la Escuela de Informática.

Este programa de técnico corresponde al Estándar de Cualificación de Ciberseguridad 0612-14-03-3-01.

El programa constará en nueve bimestres. Con excepción del último de ellos, cada bimestre tendrá dos cursos de Ciberseguridad de 96 horas cada uno, y uno de inglés de 64 horas. De esta manera, el total de los primeros ocho bimestres será de 2048. El último bimestre tendrá un total de horas de 320. El total de horas del programa de técnico será de 2368. La modalidad del programa es mixta [2] (presencial y virtual). Los cursos contemplan tanto horas contacto (lectivas) como horas de trabajo independiente del estudiante. La estructura curricular se muestra en el Anexo A, y en el Anexo B se presentan los programas de los cursos.

3. Objeto de estudio

La Escuela de Informática define la ciberseguridad de la siguiente manera:

> La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es un factor clave que no puede desligarse del área de negocio. Se trata de la parte relacionada con la informática que se enfoca en la protección de los equipos, dispositivos, sistemas, redes, información y datos de cualquier ataque malicioso. En resumen, no es más que la seguridad de las tecnologías de la información, es decir, tratar de mitigar todos los riesgos que una organización pueda tener en la red. Su principal objetivo es evitar que las amenazas cibernéticas pongan en peligro la información de una organización. Así, la ciberseguridad comprende la protección de software (bases de datos, archivos, redes…), hardware y todo aquello que una organización valore como un riesgo si esa información cae en manos de otras personas. Para ello existen una serie de estándares, protocolos, métodos, reglas y herramientas que han sido concebidos para minimizar los posibles riesgos en las infraestructuras y en la propia información. (Universidad Nacional, DC-01 Información general del programa de técnico en Ciberseguridad, 2024).

4. Propósitos

El propósito general del Técnico 3 en Ciberseguridad es el siguiente:

> Formar técnicos en Ciberseguridad para la ejecución, instalación, configuración, monitoreo y diagnóstico de los sistemas de información, con una sólida base integral de conocimientos, habilidades, actitudes y valores éticos en la aplicación de soluciones de defensa y respuesta a incidentes para la protección de los activos informáticos de las organizaciones, según la legislación y políticas de seguridad vigentes. (Universidad Nacional, FR MNC Tabla comparativa Contenido Diseño curricular, Técnico en Ciberseguridad, 2024).

[2] Definición de mixta: Las personas estudiantes realizan sus procesos de aprendizaje de manera tal que se combinan sesiones virtuales y presenciales, con mediación docente, utilizando campus virtuales y herramientas de comunicación; además, tomando en consideración que las sesiones presenciales requieren un espacio físico (aula, laboratorio, taller u otro).

5. Requisitos de ingreso

Los requisitos académicos de ingreso al Técnico 3 en Ciberseguridad es poseer al menos el Bachillerato en Educación Media. Esto está de acuerdo con lo establecido en el estándar específico de Técnico en Ciberseguridad 0612-14-03-3-01.

6. Justificación

Lo siguiente son extractos de la justificación que envió la Universidad Nacional:

> El aumento de las amenazas cibernéticas ha creado una demanda sin precedentes de los técnicos especialistas a nivel global. Las filtraciones de datos, las infecciones de malware (programas malignos) y las vulnerabilidades de software son comunes en la tecnología actual y es fundamental comprender completamente cómo ocurren estos ataques, cómo prevenirlos y cómo recuperarse. La Ciberseguridad se ha convertido en un aspecto clave y de primera necesidad en la estrategia de todas las organizaciones.
> Ante una era cada vez más digital en la que la tecnología ha cobrado un papel primordial, se hace imprescindible que una organización tenga claro el equilibrio entre la seguridad, la funcionalidad de los productos o servicios, el tratamiento de la información y los riesgos que pueden derivar.
> Los técnicos en Ciberseguridad tienen la necesidad de interactuar con las diversas disciplinas que existen en el campo de las Tecnologías de Información y Comunicaciones. Esta carrera en modalidad bimodal (presencial-virtual), representa el vehículo adecuado, para lograr la integración de las diferentes áreas con los saberes cognitivos, las habilidades técnicas y las blandas, así como las actitudes (saber ser y convivir juntos) de las Tecnologías de Información y Comunicaciones, para asegurar en diferentes ámbitos a las organizaciones y anticiparse a los impactos que los eventos nacionales o internacionales, pueda tener en sus organizaciones.
> Según el más reciente informe de la OIT: Perspectivas Sociales y del Empleo en el Mundo, 20211, las plataformas digitales de trabajo se han multiplicado por cinco en el último decenio y están abriendo nuevas posibilidades, en particular, para las mujeres, las personas con discapacidad, los jóvenes y las personas que quedan al margen de los mercados laborales convencionales. A las empresas, las plataformas les permiten acceder a una base de trabajadores amplia, flexible y con calificaciones diversas, además de ampliar su base de clientes.
> Los avances tecnológicos –la inteligencia artificial, la automatización, la robótica, la *big data*, el comercio electrónico – crearán nuevos puestos de trabajo que den soporte a la industria, y todos ellos requieren de la seguridad informática porque hay que considerar esa temática en los programas, en las conexiones, en las comunicaciones, en lo que se aloja en la nube y lograr procesos de transformación seguros.
> A partir del 2017, con la consolidación de los modelos de negocios usando plataformas basadas en tecnología (Fintech), así como la aparición del Blockchain o cadena de bloques, el manejo de volúmenes de datos y la inteligencia artificial trajeron grandes cambios al sector financiero, al igual que el comercio electrónico y con ello la incorporación de la seguridad informática en estos procesos para asegurar que los procesos sensibles no se comprometan, que la información sea fidedigna y resguardada efectivamente por quienes corresponda
> Estas son áreas modernas de las tecnologías de información que aparece incluso como uno de los nuevos pilares de las ciencias de la computación a nivel mundial, como se destaca en los informes de la Association for Computing Machinery (ACM) en 2017. Esta organización proyecta para el 2022 una demanda aguda no satisfecha a nivel mundial de millones de puestos relativos a la seguridad informática y el último reporte del 2020

incorpora las áreas de seguridad informática o ciberseguridad y ciencia de datos como nuevos pilares de las ciencias de la computación.
Aun así, según el Informe sobre Madurez Digital en Ciberseguridad 2021-20212, elaborado por Minsait y SIA, la madurez en materia de ciberseguridad ha dividido el tejido empresarial en dos grupos diferenciados: los que temen las consecuencias y los que no. Así es como un 56% de las empresas carece de una estrategia de ciberseguridad bien definida a pesar de conocer los problemas que podría acarrear un ataque de estas magnitudes. El informe también revela que el 73% de las empresas no cuenta con los mecanismos de incentivos, formación y comunicación precisos para sus profesionales que faciliten un cambio necesario en la organización en materia de ciberseguridad.
Definir mecanismos de seguridad y establecer protocolos de actuación ante los ciberataques han sido importantes siempre, pero hoy en día este aspecto cobra especial relevancia, sobre todo desde el arranque de la pandemia, con el que la mayoría de las empresas se han visto obligadas a implantar el trabajo en remoto y muchas han potenciado los canales de venta en línea, multiplicando el riesgo de sufrir un ciberataque que ponga en peligro su actividad. (Universidad Nacional, DC-01 Información general del programa de técnico en Ciberseguridad, 2024).

Esta Oficina considera que la justificación anterior es apropiada.

7. Alineación de la propuesta curricular con el estándar de cualificación

La propuesta curricular es congruente con lo planteado en el estándar de cualificación asociado.

8. Cumplimiento de horas de la propuesta curricular en relación con el nivel de técnico estipulado por el MNC-EFTP-CR

Según la normativa vigente, un programa de Técnico de Nivel 3 debe cumplir con un rango de horas entre 2300 a 2849 horas. La propuesta curricular contempla 2368 horas; por lo tanto, se cumple con lo establecido en la normativa.

9. Correspondencia de las competencias con el estándar de cualificación

COMPETENCIA GENERAL:
Ejecutar la instalación, configuración, monitoreo y diagnóstico de los sistemas de información, aplicando soluciones de defensa y respuesta a incidentes para proteger los activos informáticos de la organización, según la legislación nacional e internacional y políticas de seguridad vigentes; actuando con ética a nivel personal, profesional y laboral, coordinando con los niveles jerárquicos de la organización la solución de problemas

COMPETENCIAS ESPECIFICAS

Competencia Especifica (CE) 1:

Instalar y configurar equipo activo en la red de comunicación de datos, de acuerdo con normativa y políticas de seguridad del entorno organizacional

Resultados de aprendizaje asociados a la anterior competencia específica:

La persona es competente cuando:
1. Instala equipo activo en la red de comunicación.
2. Configura el equipo activo en la red de comunicación.
3. Diagnostica fallas en los equipos activos en la red de comunicación.
4. Corrige fallas en los equipos activos en la red de comunicación.
5. Aplica a la red de comunicación la normativa y políticas de seguridad del entorno organizacional.

Contenido asociado a los anteriores resultados de aprendizaje:

Introducción a las redes:
Tema 1. Las redes en la actualidad
Tema 2. Configuración básica de switches y dispositivos
Tema 3. Protocolos y modelos
Tema 4. Capa física
Tema 5. Sistemas numéricos
Tema 6. Capa de enlace de datos
Tema 7. Switching Ethernet
Tema 8. Capa de red
Tema 9. Resolución de dirección
Tema 10. Configuración básica de un router
Tema 11. Asignación de direcciones IPv4
Tema 12. Asignación de direcciones IPv6
Tema 13. ICMP
Tema 14. Capa de transporte
Tema 15. Capa de aplicación
Tema 16. Fundamentos de seguridad de la red
Tema 17. Crear una red pequeña

Fundamentos de conmutación, enrutamiento y redes inalámbricas:
Tema 1. Configuración básica de dispositivos
Tema 2. Conceptos de switching
Tema 3. VLAN
Tema 4. Enrutamiento entre VLAN
Tema 5. STP
Tema 6. Etherchannel
Tema 7. DHCPv4
Tema 8. Conceptos de SLAAC y DHCPv6
Tema 9. Conceptos de FHRP
Tema 10. Conceptos de seguridad de LAN
Tema 11. Configuración de seguridad de switch
Tema 12. Conceptos de WLAN
Tema 13. Configuración de WLAN
Tema 14. Conceptos de enrutamiento
Tema 15. Rutas IP estáticas
Tema 16. Resolución de problemas de rutas estáticas y predeterminadas"

Laboratorio y herramientas para ciberataques:
Tema 1: Herramientas para utilizar en cada etapa del proceso de un ataque.
Tema 2: Herramientas para la protección de la infraestructura de una organización.
Tema 3: Principales herramientas utilizadas por el equipo rojo y azul.
Tema 4: Desarrollo de laboratorio final.

Informática forense:
Tema 1: Fundamentos de informática forense
Tema 2: Identificación
Tema 3: Preservación
Tema 4: Análisis y presentación de la Evidencia

Práctica profesional:
Contenidos del Seminario de Ciberseguridad
Contenidos de la Práctica Supervisada en Ciberseguridad

Competencia Especifica (CE) 2:

Instalar sistemas operativos de código abierto y propietario, asimismo configurar servicios para la red de comunicación, de acuerdo con normativa y políticas de seguridad de la organización.

Resultados de aprendizaje asociados a la anterior competencia específica:

La persona es competente cuando:
1. Instala sistemas operativos de código abierto y propietario.
2. Configura servicios para la red de comunicación de datos en sistemas operativos de código abierto y propietario.
3. Diagnostica fallas en sistemas operativos y servicios de la red de comunicación de datos.
4. Corrige fallas en sistemas operativos y servicios de la red de comunicación de datos.
5. Aplica la normativa y políticas de seguridad establecidas a nivel nacional e internacional y de la organización.

Contenido asociado a los anteriores resultados de aprendizaje:

Sistemas operativos aplicados:
Tema 1. Conceptos básicos de sistemas operativos.
Tema 2. Estructuras de los sistemas operativos.
Tema 3. Manejo del CLI.
Tema 4. Utilidades del sistema.
Tema 5. Control de acceso.
Tema 6. Mantenimiento del sistema.
Sistemas operativos para dispositivos móviles:
Tema 1: Fundamentos de Sistemas Operativos Móviles en la actualidad.
Tema 2: Principales amenazas y vulnerabilidades en entornos móviles.
Tema 3: Herramientas para la administración y detección de amenazas móviles.
Tema 4: Aspectos de resiliencia en dispositivos móviles.
Laboratorio y herramientas para ciberataques:
Tema 1: Herramientas para utilizar en cada etapa del proceso de un ataque.
Tema 2: Herramientas para la protección de la infraestructura de una organización.
Tema 3: Principales herramientas utilizadas por el equipo rojo y azul.
Tema 4: Desarrollo de laboratorio final.
Informática forense:

Tema 1: Fundamentos de informática forense
Tema 2: Identificación
Tema 3: Preservación
Tema 4: Análisis y presentación de la Evidencia"
Práctica profesional:
Contenidos del Seminario de Ciberseguridad Contenidos de la Práctica Supervisada en Ciberseguridad

Competencia Especifica (CE) 3:
Realizar monitoreo y diagnóstico de la seguridad de los sistemas de información, según la legislación nacional e internacional y políticas de seguridad vigentes.

Resultados de aprendizaje asociados a la anterior competencia específica:
La persona es competente cuando:
1. Desarrolla código scripting utilizando un lenguaje de programación y técnicas de codificación vigentes.
2. Identifica métodos de evasión y ofuscación, según especificaciones técnicas.
3. Aplica protocolos de protección a los sistemas de información, según normativas vigentes y estándares internacionales.
4. Diagnostica procesos de autentificación y autorización entre dispositivos de usuario final y recursos de red informáticos, según políticas organizacionales.
5. Explica el funcionamiento de componentes de los sistemas digitales utilizando el sistema operativo correspondiente y especificaciones del fabricante.
6. Configura componentes de los sistemas digitales, según especificaciones técnicas.
7. Aplica soluciones de integridad, confidencialidad y disponibilidad en las transacciones web, según requerimiento organizacional.
8. Analiza el tráfico de red y su comportamiento, según las políticas de seguridad.
9. Identifica vulnerabilidades en las aplicaciones, según los requerimientos organizacionales.
10. Explica mecanismos de seguridad en dispositivos móviles, según requerimientos organizacionales.
11. Genera informes sobre la seguridad de las aplicaciones, con base en la legislación vigente y las políticas organizacionales.

Contenido asociado a los anteriores resultados de aprendizaje:

Introducción a la seguridad de la información:
Tema 1: Fundamentos de Ciberseguridad.
Tema 2: Tipos de amenazas, vulnerabilidades y ataques de ciberseguridad.
Tema 3: Infraestructura de la ciberseguridad.
Tema 4: Procesos, estándares y dispositivos de seguridad.
Legislación en ciberseguridad:
Tema 1: Ley 9048 de Delitos Informáticos.
Tema 2: Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.
Tema 3: GDPR (Unión Europea).
Tema 4: Regulación americana de protección de datos.
Programación en Python:
Tema 1: Estrategias y métodos para resolver problemas.
Tema 2: Estructuras y tipos de datos.
Tema 3: Colecciones básicas.

Ética de la ciberseguridad:
Tema 1. Introducción a la ética en la ciberseguridad.
Tema 2. Consecuencias éticas y morales de los ataques cibernéticos.
Tema 3. Implementación práctica de los códigos de ética.
Tema 4. Interacción efectiva y ética para las relaciones laborales, profesionales y personales.

Ingeniería social:
Tema 1: Etapas de un ataque de ingeniería social.
Tema 2: Creación de ataques de ingeniería social.
Tema 3: Defensas de ataques de ingeniería social.
Estándares de seguridad de la información:
Tema 1: Clasificación de datos.
Tema 2. Análisis de estándares de seguridad de la información.
Tema 3. Políticas y procesos de aplicación
Análisis de software malicioso:
Tema 1. Introducción a la clasificación de programas maliciosos.
Tema 2. Arquitectura básica de un ataque informático.
Tema 3. Herramientas de análisis de programas maliciosos.
Tema 4. Análisis forense básico contra software malicioso
Metodologías y ciclo de vida de los ciberataques:
Tema 1: Fases del Hacking ético.
Tema 2: Metodología de Cyber Kill Chain.
Tema 3: Prevención y mitigación.
Laboratorio y herramientas para ciberataques:
Tema 1: Herramientas para utilizar en cada etapa del proceso de un ataque.
Tema 2: Herramientas para la protección de la infraestructura de una organización.
Tema 3: Principales herramientas utilizadas por el equipo rojo y azul.
Tema 4: Desarrollo de laboratorio final.
Informática forense:
Tema 1: Fundamentos de informática forense
Tema 2: Identificación
Tema 3: Preservación
Tema 4: Análisis y presentación de la Evidencia

Práctica profesional:
Contenidos del Seminario de Ciberseguridad
Contenidos de la Práctica Supervisada en Ciberseguridad

Competencia Especifica (CE) 4:

Implementar técnicas para la defensa de infraestructura de información, según la legislación nacional e internacional y políticas de seguridad vigentes.

Resultados de aprendizaje asociados a la anterior competencia específica:

La persona es competente cuando:
1. Interpreta fases de la ciberseguridad, según los requerimientos organizacionales y políticas de seguridad vigentes.

2. Implementa normas de seguridad en los sistemas de información, según la legislación nacional e internacional y políticas de seguridad vigentes.
3. Aplica técnicas de Ingeniería Social para la defensa de infraestructuras de información, según los requerimientos organizacionales.
4. Ejecuta planes remediales para corrección de situaciones de vulnerabilidad, según los requerimientos organizacionales.

Contenido asociado a los anteriores resultados de aprendizaje:
Legislación en ciberseguridad:
Tema 1: Ley 9048 de Delitos Informáticos.
Tema 2: Ley de Protección de la persona frente al tratamiento de sus datos personales.
Tema 3: GDPR (Unión Europea).
Tema 4: Regulación americana de protección de datos.
Ética de la ciberseguridad:
Tema 1. Introducción a la ética en la ciberseguridad.
Tema 2. Consecuencias éticas y morales de los ataques cibernéticos.
Tema 3. Implementación práctica de los códigos de ética.
Tema 4. Interacción efectiva y ética para las relaciones laborales, profesionales y personales.

Ingeniería social:
Tema 1: Etapas de un ataque de ingeniería social.
Tema 2: Creación de ataques de ingeniería social.
Tema 3: Defensas de ataques de ingeniería social.
Estándares de seguridad de la información:
Tema 1: Clasificación de datos.
Tema 2. Análisis de estándares de seguridad de la información.
Tema 3. Políticas y procesos de aplicación
Gestión de riesgos empresariales:
Tema 1. Aseguramiento de la información.
Tema 2. Matriz de riesgos.
Tema 3. Gestión de riesgos
Seguridad del software (OWASP):
Tema 1. Introducción a la seguridad del software.
Tema 2: Análisis de vulnerabilidades del Top 10 de OWASP Web.
Tema 3: Análisis de vulnerabilidades dl OWASP Móviles
Laboratorio y herramientas para ciberataques:
Tema 1: Herramientas para utilizar en cada etapa del proceso de un ataque.
Tema 2: Herramientas para la protección de la infraestructura de una organización.
Tema 3: Principales herramientas utilizadas por el equipo rojo y azul.
Tema 4: Desarrollo de laboratorio final.
Informática forense:
Tema 1: Fundamentos de informática forense
Tema 2: Identificación
Tema 3: Preservación
Tema 4: Análisis y presentación de la Evidencia"

Práctica profesional:
Contenidos del Seminario de Ciberseguridad
Contenidos de la Práctica Supervisada en Ciberseguridad

ÁMBITO LABORAL

La Universidad Nacional envió la siguiente información sobre el particular:

> Con la carrera de Técnico en Ciberseguridad se tendrán profesionales aptos para desarrollarse en forma integral dentro del área de ciberseguridad con conocimientos teóricos-prácticos y una serie de habilidades y valores que los potencializarán como líderes en el campo de la ciberseguridad ya que serán capaces de concatenar personas e ideas que logren soluciones prácticas de beneficio a todos los participantes; innovaciones coherentes con la ética y profesionalismo en la aplicación de las herramientas tecnológicas.
> Los graduados pueden ocupar puestos de trabajo tales como:
> - Asistente del coordinador de las áreas de seguridad informática o ciberseguridad en organizaciones autónomas, gubernamentales o no gubernamentales y empresas privadas para la detección de fallas de seguridad.
> - Encargado de la protección de la información en redes informáticas, sistemas operativos, sistemas de información de las organizaciones.
> - Encargado de análisis forense y análisis malware
>
> Para estas funciones es necesario que tenga capacidad para la ejecución de algunas tareas específicas relacionadas con:
>
> - Instalación y configuración de equipos activos en las redes de comunicación de datos, de acuerdo con normativa y políticas de seguridad del entorno organizacional.
> - Instalación de sistemas operativos de código abierto y propietario de acuerdo con normativa y políticas de seguridad de la organización.
> - Configuración de los servicios para las redes de comunicaciones, de acuerdo con normativa y políticas de seguridad de la organización.
> - Tareas de monitoreo y diagnóstico de la seguridad de los sistemas de información, según la legislación nacional e internacional y políticas de seguridad vigentes.
> - Aplicar diferentes técnicas para la defensa de infraestructura de información, según la legislación nacional e internacional y políticas de seguridad vigentes.
>
> Este profesional se distinguirá en las organizaciones por sus calidades profesionales y humanas, su clara ética en el desempeño laboral, sensibilidad social y capacidad de apoyar el aporte de soluciones a los problemas detectados en los procesos de ciberseguridad.

10. Estrategias metodológicas de mediación

Sobre el particular, la Universidad Nacional señala lo siguiente para los cursos de Informática:

> La participación del estudiante durante el curso bimodal es de gran importancia para lograr las competencias. Las actividades programadas son formativas y participativas por lo que cada alumno tiene la posibilidad de expresar sus ideas, opiniones, críticas y análisis. La experiencia de los estudiantes se enriquece a través de las lecturas y el análisis de materiales audiovisuales, así como actividades tanto individuales como grupales lo que permite forjar mentes abiertas para ser profesionales con mejores habilidades empresariales, administrativas y sociales. Se aplican con rigurosidad las revisiones del trabajo, sesiones de retroalimentación y evaluación continua formativa, incluso entre pares, a través de foros abiertos de crítica y autocrítica. (Universidad Nacional, Escuela de Informática, Tomo curricular con los programas, Técnico en Ciberseguridad, 2023).

En cuanto a los cursos de inglés y su estrategia metodológica, la Universidad Nacional señala lo siguiente:

> Las clases se desarrollan con el apoyo de herramientas y plataformas tecnológicas. Se utiliza la serie de libros *Outstanding!* como texto de apoyo para el desarrollo de los contenidos. Este nivel está fundamentado en la metodología comunicativa (CLT) lo que promueve un aprendizaje interactivo y eficiente para la persona usuaria. Bajo esta corriente pedagógica la persona usuaria es protagonista principal en la construcción de su propio aprendizaje; la persona docente, en su papel de guía y facilitador, se encarga de propiciar el ambiente adecuado y las condiciones necesarias para el uso intensivo del idioma, por medio de actividades individuales, en parejas o grupales. Las actividades están dirigidas a integrar las cuatro habilidades principales del idioma más la gramática. La persona docente brinda apoyo especial para fortalecer el proceso de enseñanza-aprendizaje de la persona usuaria. (Universidad Nacional, Escuela de Informática, Tomo curricular con los programas, Técnico en Ciberseguridad, 2023).

11. Correspondencia del equipo docente con las actividades académicas

La unidad académica a cargo envió a esta Oficina una nota (ver anexo C) en la cual certifica que los requisitos con los que deben contar los docentes para ser parte del programa son los siguientes:

- Poseer al menos un Bachillerato en “Ingeniería en informática, computación, ingeniería en sistemas, sistemas de Información, sistemas WEB administración de proyectos, gestión de proyectos, tecnologías de la información, auditoría de tecnologías y sistemas de información, análisis de datos, telemática, ciberseguridad, análisis de sistemas, bases de datos, servidores web libres, programación, ingeniería de software, electrónica [u] otra carrera atinente al curso por impartir”
- Contar con una experiencia laboral de al menos un año en el área en que va a enseñar.
- Contar con una experiencia docente de al menos seis meses.

12. Conclusiones

La propuesta cumple con la normativa aprobada por el CONARE en relación con los procedimientos establecidos por el documento *Lineamientos para la revisión curricular por parte de OPES de los programas de Educación y Formación Técnica Profesional en las universidades estatales.* Por lo tanto, la División Académica de la OPES avala para que el MNC-EFTP brinde la alineación del programa con el estándar correspondiente según lo

estipulado en este dictamen y autoriza a la Escuela de Ciberseguridad de la Universidad Nacional para que imparta el programa de Técnico 3 en Ciberseguridad.

13. Anexos

ANEXO A

ESTRUCTURA CURRICULAR DEL TÉCNICO EN CIBERSEGURIDAD DE LA UNIVERSIDAD NACIONAL

BIMESTRE Y CURSO	HORAS
I BIMESTRE	256
Introducción a las redes	96
Introducción a la seguridad de la información	96
Inglés 1	64
II BIMESTRE	256
Fundamentos de conmutación, enrutamiento y redes inalámbricas	96
Legislación en ciberseguridad	96
Inglés 2	64
III BIMESTRE	256
Sistemas operativos aplicados	96
Programación en Python	96
Inglés 3	64
IV BIMESTRE	256
Sistemas operativos para dispositivos móviles	96
Ética de la ciberseguridad	96
Inglés 4	64
V BIMESTRE	256
Ingeniería social	96
Estándares de seguridad de la información	96
Inglés 5	64
VI BIMESTRE	256
Análisis de software malicioso	96
Gestión de riesgos empresariales	96
Inglés 6	64

BIMESTRE Y CURSO	HORAS
VII BIMESTRE	256
Seguridad del software (OWASP)	96
Metodologías y ciclo de vida de los ciberataques	96
Inglés 7	64
VIII BIMESTRE	256
Laboratorio y herramientas para ciberataques	96
Informática forense	96
Inglés 8	64
IX BIMESTRE	320
Práctica profesional	320
Total de horas del Técnico en Ciberseguridad	***2368***

ANEXO B

DESCRIPCIÓN DE LOS MÓDULOS DEL PROGRAMA DE TÉCNICO EN CIBERSEGURIDAD DE LA UNIVERSIDAD NACIONAL

1. Introducción a las redes.

Descripción del curso:
Este curso presenta la arquitectura, la estructura, las funciones, los componentes y los modelos de Internet y de otras redes informáticas. A modo de base para el currículo, se presentan los principios y la estructura del direccionamiento IP y los aspectos fundamentales de los conceptos, los medios y las operaciones de Ethernet. Para el final del curso, los estudiantes serán capaces de construir redes LAN simples, realizar configuraciones básicas para routers y switches e implementar esquemas de direccionamiento IP.
Este curso corresponde al técnico en Ciberseguridad, y al área de **Normas y políticas de seguridad**, se impartirá de forma mixta, con una metodología dinámica donde las actividades están centradas en el quehacer del estudiante, concibiendo al docente como un guía-tutor en el desarrollo del proceso de aprendizaje del estudiante, y siempre teniendo en mente la siguiente pregunta:
Contenidos:
Tema 1. Las redes en la actualidad

a. Componentes de la red
b. Topologías y representaciones de red
c. Tipos comunes de redes

Tema 2. Configuración básica de switches y dispositivos

a. La estructura de los comandos
b. Acceso a la terminal
c. Gestión de los archivos de configuración

Tema 3. Protocolos y modelos

a. Suites de protocolos
b. Organizaciones de estándares
c. Modelos de referencia
d. Encapsulamiento de datos

Tema 4. Capa física

a. Características de la capa física
b. Medios de transmisión en la red

Tema 5. Sistemas numéricos

a. Sistemas decimal, binario y hexadecimal
b. Conversión entre sistemas

Tema 6. Capa de enlace de datos

a. Características y funcionamiento
b. Formato de trama

Tema 7. Switching Ethernet

a. Tramas Ethernet
b. Direccionamiento MAC

Tema 8. Capa de red

a. Paquetes IPv4 e IPv6
b. Introducción al enrutamiento

Tema 9. Resolución de dirección

a. ARP
b. Detección de vecinos IPv6

Tema 10. Configuración básica de un router

a. Configuración de los parámetros iniciales
b. Configuración de interfaces
c. Gateway predeterminado

Tema 11. Asignación de direcciones IPv4

a. Estructura de la dirección IPv4
b. Tipos de direcciones
c. Segmentación de la red y subredes

Tema 12. Asignación de direcciones IPv6

a. Tipos de direcciones IPv6
b. Direcciones IPv6 de multidifusión
c. División de subredes IPv6

Tema 13. Protocolos de mensajes de control de Internet (ICMP)

a. Mensajes ICMP
b. Utilidades para la verificación del funcionamiento de la red

Tema 14. Capa de transporte

a. Descripción general de TCP y UDP
b. Proceso de comunicación TCP
c. Proceso de comunicación UDP
d. Números de puerto

Tema 15. Capa de aplicación

a. Protocolos web y correo electrónico
b. Servicios de direccionamiento IP
c. Servicios de intercambio de archivos

Tema 16. Fundamentos de seguridad de la red

a. Vulnerabilidades y amenazas a la seguridad
b. Ataques de red
c. Seguridad de los dispositivos

Tema 17. Crear una red pequeña

a. Protocolos y aplicaciones
b. Escalabilidad de redes

c. Técnicas de resolución de problemas

2. Introducción a la seguridad de la información.

Descripción del curso:
En la década de los setenta se crearon las primeras computadoras personales y se vende el sueño de los beneficios y comodidades que representará la tecnología en la humanidad. Cincuenta años después, estos dispositivos se han convertido en compañeros indispensables, facilitando el día a día y albergando más capacidad de procesamiento, que la necesaria para llevar a la humanidad a la luna.
Estas facilidades, han creado enormes amenazas a la privacidad, integridad y seguridad de la población, al permitir que atacantes anónimos se apoderen de información sensible, bloquen servicios, rapten infraestructura, expongan información personal, sensible o confidencial y amenacen la integridad, reputación o el negocio de empresas enteras.
Por esta razón, nace la necesidad de desarrollar profesionales en el área de informática especializados en la ciberseguridad, con capacidad de reconocer amenazas, ataques o vulnerabilidades en una organización, liderar propuestas o iniciativas para disminuir la superficie de riesgo a una amenaza y establecer parámetros que indiquen la base de seguridad de ésta.
Según el perfil profesional, los participantes dominarán los conceptos básicos de ciberseguridad y diferenciarán los tipos de amenazas para una organización, reconocen las discordancias entre los tipos de software malicioso, ataques, principales vulnerabilidades, y técnicas utilizadas por los ciber-delincuentes para completar su intención.
Contenidos:
Tema 1: Fundamentos de Ciberseguridad.
- Conceptos básicos de la seguridad: Framework, ataque, riesgo, amenaza, entre otros
- Tipos de atacantes y organizaciones
- Roles y tareas dentro de un Centro de Operaciones de Seguridad
- Protocolos de red relacionados a la seguridad

Tema 2: Tipos de amenazas, vulnerabilidades y ataques de ciberseguridad.
- Tipos de software malicioso
- Tácticas y estrategias de los atacantes
- Manejo correcto de vulnerabilidades

Tema 3: Infraestructura de la ciberseguridad.
- Topologías
- Infraestructura de seguridad: física, lógica, seguridad por capas, perimetral
- Herramientas de ciberseguridad
- Estándares y protocolos

Tema 4: Procesos, estándares y dispositivos de seguridad.
- Procesos de seguridad
- Normas de seguridad
- Dispositivos de seguridad
- Criptografía básica

3. Programa de Cursos Libres de Inglés Conversacional

Descripción del curso:
Este es el nivel 1 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de

acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso al igual que la gramática. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de guiar a los estudiantes de un nivel cero de conocimiento del idioma hacia un nivel de competencia de Beginner A1.1 según el MCERL.

Temática:

1. **Nice to Meet you!**
    a. Alfabeto, números, fechas y vocabulario simple
    b. Entender y usar presentaciones personales básicas, saludos y despedidas
    c. Preguntar y responder preguntas personales simples
    d. Descripción propia y de terceras personas
    e. Países y nacionalidades
    f. Verbo “to be” y reducciones
    g. Presente Simple
    h. Adjetivos posesivos
2. **My Family**
    a. Miembros de la familia
    b. Apariencia personal
    c. Preguntar y responder preguntas personales simples
    d. Demostrativos
    e. How many, some, any, who,
    f. Adjetivos posesivos
    g. Preposiciones de lugar
    h. Artículo indefinido (a, an) / definido (the)
    i. Uso del “There is/There are”
3. **What fruits do you like?**
    a. Vocabulario de frutas y vegetales
    b. Uso del *this, that, these, those*
    c. Wh-questions
    d. Yes/no questions
    e. Recetas de ensaladas, cantidades
4. **The Weather**
    a. Tipos de clima
    b. Predecir el clima
    c. Presente simple
    d. preguntas simples afirmativas y negativas
    e. preguntas de información
    f. Adjetivos
5. **Shopping Around**
    a. Vocabulario de prendas de vestir
    b. Precios
    c. Cantidades
    d. Colores
    e. Tipos de ropa
    f. Uso del *what* y *which*
6. **Sports**
    a. Vocabulario de deportes
    b. Uso del *like*
    c. Uso del *why*

d. Hablar sobre deportes favoritos
e. Revisión desde los fundamentos hasta lo visto en la unidad 6

4. Fundamentos de conmutación, enrutamiento y redes inalámbricas

Descripción del curso:

Este curso se enfoca en tecnologías de switching y operaciones de los router que soportan redes empresariales pequeñas y medianas, y según el perfil profesional se incluye el dominio de conceptos de seguridad en la red y tecnologías inalámbricas (WLAN), además los estudiantes serán capaces de realizar la configuración básica de una red y aplicar mecanismos de resolución de problemas, identificar y mitigar amenazas de seguridad en la LAN y configurar y asegurar una WLAN.

Contenidos:

Tema 1. Configuración básica de dispositivos

d. Acceso remoto seguro
e. Configuración básica de switch
f. Configuración básica de router

Tema 2. Conceptos de switching

d. Reenvío de tramas
e. Direccionamiento MAC
f. Dominios de switching

Tema 3. VLAN

e. Descripción general de las VLAN
f. Configuración de VLAN
g. Enlaces troncales
h. Protocolo de enlace troncal dinámico

Tema 4. Enrutamiento entre VLAN

c. Funcionamiento de Inter-VLAN routing
d. Resolución de problemas de Inter-VLAN routing

Tema 5. STP

c. Propósito y funcionamiento de STP
d. Evolución de STP

Tema 6. Etherchannel

c. Configuración y funcionamiento
d. Verificación y solución de problemas de Etherchannel

Tema 7. DHCPv4

c. Conceptos y proceso de asignación de direcciones dinámicamente
d. Configuración de un servidor DHCPv4

Tema 8. Conceptos de SLAAC y DHCPv6

c. SLAAC
d. DHCPv6

Tema 9. Conceptos de FHRP

c. Protocolos de redundancia de primer salto
d. HSRP

Tema 10. Conceptos de seguridad de LAN

d. Control de acceso
e. Amenazas a la seguridad de capa 2
f. Ataques a la LAN

Tema 11. Configuración de seguridad de switch

d. Implementación de seguridad en puertos
e. Mitigación de ataques a VLAN, DHCP, ARP y STP

Tema 12. Conceptos de WLAN

d. Componentes de una WLAN
e. Administración de canales
f. WLAN seguras

Tema 13. Configuración de WLAN

c. Configuración de una WLAN básica
d. Solución de problemas de WLAN

Tema 14. Conceptos de enrutamiento

e. Reenvío de paquetes
f. Tabla de routing IP
g. Enrutamiento estático y dinámico

Tema 15. Rutas IP estáticas

d. Configuración de rutas estáticas IP
e. Configuración de rutas estáticas predeterminadas
f. Configuración de rutas estáticas flotantes

Tema 16. Resolución de problemas de rutas estáticas y predeterminadas

d. Procesamiento de paquetes en rutas estáticas
e. Proceso de diagnóstico y resolución de problemas en rutas estáticas

5. Legislación en ciberseguridad.

Descripción del curso:

Este curso tiene como fin conocer el marco legal, tanto nacional como internacional, que tiene impacto en el manejo de los datos, seguridad de datos, análisis de actividad criminal, manejo de evidencia, así como la protección de identidad de las personas o empresas.

Recién se comienza a instaurar la legislación para el mundo cibernético, en el cual se depende del internet, de la velocidad y seguridad del manejo de datos y la garantía de que la información personal no se vea afectada por un tercero con intenciones malignas. La instauración de diferentes leyes a lo largo de los últimos 25 años ha llegado a ser la prioridad para entes gubernamentales y privados.

En Costa Rica, se creó la Ley N° 8148 de Delitos Informáticos en el año 2001, estudiar y aprender la legislación nacional es el primer paso para aprender el marco legal ante el manejo de acceso de datos, robo de información, piratería.

En los Estados Unidos, las leyes de ciber seguridad van desde el nivel federal, estatal y municipal; también se considera de importancia la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPPA por sus siglas en inglés) que tiene una serie de estándares normativos que obliga a las empresas que tratan información médica protegida a implementar y seguir medidas de seguridad física para sus redes y procesos. También se encuentra la Comisión Federal de Comercio (FTC) cuyo objetivo es proteger a los

consumidores, prevenir el fraude, el engaño y las prácticas comerciales desleales en el mercado.
En la Unión Europea, la Regulación General de la Protección de Datos (GDPR siglas en inglés) tiene como objetivo proteger el manejo de la información de las personas ciudadanas de la Unión Europea. Es altamente restrictiva y con multas altas para las empresas si lucran con información personal de los usuarios. Los trabajos de análisis de seguridad deben entender el manejo del GDPR, como base de la importancia de la protección de datos y la consecuencia de su violación.
Acorde con el perfil profesional, el conocimiento y aplicación de las diferentes legislaciones, nacionales e internacionales, es vital para que los ciber analistas identifiquen los estándares de protección y seguridad, así como la ética del manejo de información confidencial para detectar los faltantes a la ley y se brinde colaboración con las autoridades locales e internacionales.

Contenidos.

Tema 1: Ley 9048 de Delitos Informáticos

- Artículos relacionados a corrupción
- Artículos: Daño y sabotaje
- Delitos informáticos y conexos

Tema 2: Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales

- Del Consentimiento
- De los Derechos de los Titulares y su Ejercicio
- Del Tratamiento de los Datos Personales y las Medidas de Seguridad
- De la Transferencia de Datos Personales
- De la Inscripción del Registro de Bases de Datos y Ficheros ante la Agencia

Tema 3: GDPR (Unión Europea)

- Protección de datos en la unión europea
- Responsabilidades civiles
- Normas para las empresas
- Derechos civiles

Tema 4: Regulación americana de protección de datos

- Entes reguladores
- Regulación estatal vs Regulación Federal
- Normas empresariales
- Derechos civiles

6. Programa de Cursos Libres de Inglés Conversacional.

Descripción del curso:

Este es el nivel 2 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso al igual que la gramática. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de fortalecer el nivel de competencia lingüística de Beginner A1.1 según el MCERL.

Temática:

1. Places around town
    a. Reconocer lugares de la ciudad.

b. Utilizar adecuadamente frases demostrativas en singular y plural (there is / there are) para describir lugares en la ciudad.
c. Utilizar preposiciones tales como *In / On / At* para definir la ubicación de lugares en la ciudad.
d. Utilizar preposiciones de lugar para definir la ubicación de edificios en la ciudad.
e. Hacer y responder correctamente a preguntas con *"Where"*

2. At the movies
    a. Reconocer tipos de películas.
    b. Utilizar preposiciones de tiempo *In / On / At* para hablar acerca de películas y visitas al cine.
    c. Hacer y responder correctamente a preguntas con *"When"*
    d. Dar la hora en inglés de manera correcta en conversaciones cortas.
3. I'm not Feeling Well
    a. Reconocer vocabulario relacionado con las partes del cuerpo.
    b. Uso correcto del pasado simple utilizando el verbo ser o estar (be).
    c. Uso adecuado de los verbos en pasado en su forma base y/o con verbos auxiliares.
    d. Describir de forma básica padecimientos, enfermedades o malestares generales.
4. Daily Life
    a. Describir de forma básica mi rutina diaria.
    b. Uso adecuado de adverbios de frecuencia para describir mi rutina diaria.
    c. Uso de frases adverbiales de frecuencia.
    d. Reconocer vocabulario relacionado con malestares generales y como describirlos de manera básica.
5. In the House
    a. Reconocer vocabulario acerca de las distintas partes de la casa.
    b. Uso adecuado del presente progresivo (verb + ing) tanto en oraciones positivas, negativas y preguntas para describir y consultar acerca de acciones en tiempo real.
    c. Comprender lecturas cortas acerca de diferentes aposentos de la casa y su descripción.
6. Talking on the Phone
    a. Reconocer vocabulario acerca de los días de la semana.
    b. Repaso general acerca del uso adecuado de los verbos en pasado tanto en oraciones positivas, negativas y preguntas.
    c. Describir eventos simples utilizando oraciones en tiempo pretérito.

7. Sistemas operativos aplicados

Descripción del curso:

Los programas de aplicación que ejecutan los usuarios corren sobre una gama muy amplia de dispositivos de hardware. Existen diversos fabricantes, modelos, diseños, arquitecturas, entre otros, de circuitos integrados y otros elementos que conforman los dispositivos que muestran video en una pantalla, envían datos a alta velocidad, emiten sonidos de alta fidelidad, así como complejas construcciones electrónicas que permiten el procesamiento de datos. Cabe destacar que existe un complejo controlador que se encarga de manejar las operaciones del hardware por parte de los programas de aplicación, llamado el sistema operativo.

El sistema operativo es el componente de un sistema de cómputo que se encarga de administrar los recursos de hardware, de manera que los programas se puedan ejecutar

correcta y eficientemente. Además, permite mostrar una interfaz amigable para que los programadores desarrollen código más rápidamente, evitando la complejidad subyacente de los dispositivos. También, es responsable de la protección del sistema para evitar un mal funcionamiento y posibles fallos que ocurran. Por lo tanto, existen diversos sistemas operativos para distintos sistemas electrónicos, y deben evolucionar cada día para satisfacer la demanda de los usuarios y las aplicaciones, junto con las mejoras tecnológicas y nuevos aparatos electrónicos.

En este curso y según el perfil profesional se estudiarán las características de los principales sistemas operativos (Windows / Linux), operaciones, utilidades para la identificación de problemas y depuración del sistema, así como posibles vectores de ataque que permitan a una persona no autorizada tomar el control del sistema.

Contenidos:

Tema 1. Conceptos básicos de sistemas operativos

g. Componentes
h. Elementos de Hardware y comunicación con los programas de aplicación
i. Virtualización
j. Instalación del sistema operativo Windows
k. Instalación del sistema operativo Linux

Tema 2. Estructuras de los sistemas operativos

i. Llamadas a procedimientos local y remoto
j. Procesos de inicio y mantenimiento del sistema
k. Archivos de sistema

Tema 3. Manejo del CLI

g. Uso del CMD y PowerShell en ambientes Windows
h. Uso de Bash en ambientes Linux
i. Comandos y tareas básicas para la gestión del sistema

Tema 4. Utilidades del sistema

a. Herramientas para la visualización de los recursos del sistema
b. Configuración de la red y discos duros
c. Archivos de configuración
d. Archivos de ejecución por lotes (scripts)

Tema 5. Control de acceso

a. Usuarios, grupos y políticas
b. Instalación y manejo de certificados
c. Acceso remoto

Tema 6. Mantenimiento del sistema

a. Configuración de logging e integración con otros sistemas
b. Verificación de servicios del sistema operativo

8. Programación en Python.

Descripción del curso:

Este curso introduce los conceptos más importantes para el desarrollo de componentes de software a pequeña escala, presenta las relaciones entre clases y objetos, colecciones y persistencia de los datos, los cuales le dan al estudiante una perspectiva general de la programación de aplicaciones en el paradigma de orientación a objetos, estableciendo las bases sólidas al inicio del plan de estudios.

La importancia de aprender a programar va más allá de desarrollar una aplicación con algunas especificaciones con resultados esperados, comprende el ingenio para resolver problemas mediante un pensamiento que involucra creatividad y lógica con una metodología que permite tener una solución desde lo simple a lo complejo.

Según el perfil profesional, se desarrollarán las competencias que le permitan el estudio de conocimientos y habilidades sobre los principales componentes de software, las estructuras de datos elementales, la lógica, los lenguajes de programación según la tendencia del mercado, los algoritmos que permitan resolver problemas computacionales simples, así como el conocimiento del ciclo de vida de los proyectos de programación.

Contenidos:

Tema 1: Estrategias y métodos para resolver problemas

- Diagramas de flujo
- Pseudocódigo
- Modelos matemáticos básicos
- Lógica y Operadores lógicos
- Contar

Tema 2: Estructuras y tipos de datos

- Tipos de datos abstractos
- Abstracciones comunes
- Estructuras elementales

Tema 3: Colecciones básicas

- Arreglos de tipos básicos y de objetos
- Operaciones básicas
- Bucles

Tema 4: Algoritmos

- Ordenamiento
- Búsqueda

Tema 5: Programación: Conceptos básicos

- Clase
- Objetos
- Visibilidad
- Métodos y funciones

Tema 6: Persistencia básica de datos

- Almacenamiento de los datos
- Estructura y tipos de archivos
- Recuperación de datos
- Casos de programación

9. Programa de Cursos Libres de Inglés Conversacional.

Descripción del curso:

Este es el nivel 3 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso al igual que la gramática. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de fortalecer el nivel de competencia de Elementary A1.1 según el MCERL.

Temática:

1. Greetings
    a. Reconocer saludos cotidianos que se utilizan en conversaciones a nivel básico.
    b. Reconocer vocabulario relacionado con carreras universitarias / técnicas.
    c. Hacer y responder a llamados formales.
    d. Aprender acerca de frases útiles para llamar la atención de alguien.
    e. Utilizar adecuadamente el verbo “Be” en oraciones, en preguntas abiertas (Wh-questions) o en preguntas cerradas (Yes/No Questions).
    f. Comprender lecturas cortas acerca de futuros trabajos.
    g. Escribir un correo para un amigo/conocido que reside en otro país donde se le exprese acerca de los sueños laborales a futuro.
2. Big Happy Family
    a. Utilizar correctamente preguntas simples relacionadas con miembros de la familia de forma oral.
    b. Reconocer vocabulario relacionado con los miembros de la familia extendida.
    c. Utilizar adecuadamente las formas gramaticales “Also vs. Too” de forma oral y escrita.
    d. Utilizar adecuadamente algunos intensificadores gramaticales de forma oral y escrita.
    e. Utilizar adecuadamente los adjetivos posesivos y demostrativos de forma oral y escrita.
    f. Comprender lecturas cortas acerca de la familia.
    g. Escribir acerca del árbol genealógico de una persona o de la propia familia.
3. Just for Fun
    a. Hacer y contestar correctamente preguntas simples relacionadas con pasatiempos de forma oral.
    b. Reconocer vocabulario relacionado con pasatiempos.
    c. Utilizar adecuadamente las formas gramaticales “Can vs. Can’t” de forma oral y escrita.
    d. Utilizar adecuadamente expresiones de tiempo de forma oral y escrita.
    e. Utilizar adecuadamente el tiempo presente simple en oraciones, en su forma de tercera persona del singular, y en preguntas abiertas y cerradas de forma oral y escrita.
    f. Comprender lecturas cortas acerca de pasatiempos recomendados para tener una buena salud.
    g. Escribir acerca de una rutina simple.
4. Grocery Shopping
    a. Hacer y contestar correctamente preguntas simples relacionadas con ir de compras al supermercado de forma oral.
    b. Reconocer vocabulario relacionado con artículos que venden en el supermercado.
    c. Utilizar adecuadamente adverbios de secuencia de forma oral y escrita

para dar listas de artículos que se compran en el supermercado.

- **d.** Utilizar adecuadamente preguntas de ubicación de artículos comestibles de forma oral y escrita.
- **e.** Utilizar adecuadamente los sustantivos contables y no contables tanto en singular como en plural de forma oral y escrita.
- **f.** Comprender lecturas cortas acerca de comidas y abarrotes.
- **g.** Escribir acerca de listas de compras de forma simple.

5. Blue Skies [Weather]

- **a.** Hacer y contestar correctamente preguntas relacionadas con el clima de forma oral.
- **b.** Reconocer vocabulario relacionado con el clima.
- **c.** Utilizar adecuadamente las formas gramaticales “Enough vs. Too” de forma oral y escrita.
- **d.** Hacer y responder adecuadamente preguntas de residencia y país de origen de forma oral y escrita.
- **e.** Utilizar adecuadamente los adjetivos comparativos y superlativos y sus diversas formas regulares e irregulares de forma oral y escrita.
- **f.** Comprender lecturas cortas acerca del clima.
- **g.** Escribir acerca del clima en distintas ciudades del planeta.

6. The World of Computers

- **a.** Hacer y contestar correctamente preguntas simples relacionadas con uso de las computadoras de forma oral.
- **b.** Reconocer vocabulario relacionado con el uso de la tecnología (computadoras).
- **c.** Utilizar adecuadamente las formas gramaticales “A Lot vs. A Lot of” de forma oral y escrita.
- **d.** Utilizar adecuadamente expresiones para describir problemas técnicos de forma oral y escrita.
- **e.** Utilizar adecuadamente las conjunciones de forma oral y escrita.
- **f.** Utilizar adecuadamente los verbos sensoriales de forma oral y escrita.
- **g.** Comprender lecturas cortas acerca de la tecnología y el uso del internet.
- **h.** Escribir acerca de del uso de la tecnología de forma simple.

10. Sistemas operativos para dispositivos móviles.

Descripción del curso:

Con el avance de la tecnología y del internet de las cosas, el uso de dispositivos móviles inteligentes y equipos no convencionales se torna cada vez más común, tanto en un ámbito personal como profesional, creando una necesidad urgente de administrar y proteger estos equipos de forma eficiente y agresiva, entendiendo que se han vuelto un objetivo real y alcanzable para los ciber-delincuentes.

Teniendo en cuenta la incertidumbre generada por la movilidad en la tecnología, en este curso se estudiará la arquitectura de los sistemas operativos móviles, los *firmwares* en dispositivos del internet de las cosas y el funcionamiento de los softwares relacionados a estos dispositivos. Al conocer su funcionamiento, entonces es posible entender cuáles son sus principales vulnerabilidades y crear estrategias para defenderse contra ellas, ya sean administrativas o técnicas.

Según el perfil profesional, los participantes van a ser capaces de gestionar los diferentes sistemas operativos móviles en la actualidad, así como diferenciar los alcances y amenazas a los que se encuentran expuestos. También se desarrollarán habilidades para el diseño de estrategias para la protección de la integridad de la organización, mediante políticas y acciones tanto técnicas como administrativas, disminuyendo la superficie de vulnerabilidad y creando programas mantenibles y escalables en el tiempo.

Contenidos:

Tema 1: Fundamentos de Sistemas Operativos Móviles en la actualidad.

- Conceptos básicos de los dispositivos móviles.
- Principios de amenazas y ataques hacia los dispositivos móviles
- Indicadores de riesgo y particularidades de los diferentes sistemas operativos móviles

Tema 2: Principales amenazas y vulnerabilidades en entornos móviles.

- Principales amenazas y ataques hacia los dispositivos móviles dependiendo de su sistema operativo
- Investigación y análisis de las amenazas hacia un dispositivo móvil
- Tiendas de aplicaciones
- Proceso de hackeo de dispositivos móviles

Tema 3: Herramientas para la administración y detección de amenazas móviles.

- Uso de emuladores de sistemas operativos móviles para su investigación.
- Administración de dispositivos móviles mediante el uso de Administradores de Dispositivos Móviles
- Aplicaciones para la protección de los dispositivos móviles

Tema 4: Aspectos de resiliencia en dispositivos móviles.

- Principales estrategias de resiliencia en dispositivos móviles
- Buenas prácticas para la protección de los dispositivos móviles
- Integración de los conocimientos para asegurar un entorno móvil seguro

11. Ética de la ciberseguridad.

Descripción del curso:

En este curso se propone la formación de los participantes en conocimientos y habilidades para crear una responsabilidad ética por las acciones realizadas como futuros profesionales en las diversas áreas de la ciberseguridad en que se desempeñen, a nivel empresarial y personal; y se espera la comprensión y aplicación de la ética en un alto nivel, asumiendo las consecuencias de sus actos, anteponiendo los ideales contractuales con los demás antes que sus intereses personales.

Según el perfil profesional, con la ética de la ciberseguridad se busca aplicar los valores y actitudes en todas las acciones realizadas, aún las más pequeñas, ya que en el ámbito tecnológico y social tienen consecuencias más allá de las establecidas por la ley. Esto incluye conocimientos del ámbito contractual, códigos profesionales y morales al cual se afilie el practicante de esta rama de la informática.

El curso se enfoca en formar personas que comprendan la subjetividad de la ética, practiquen lo que se considera ético dentro de un marco de un contrato laboral, y en particular a nivel de ciberseguridad. Se busca la aplicación de los conocimientos para crear mejores relaciones laborales, profesionales y personales en concordancia con las responsabilidades que le son otorgadas al ser parte de un equipo de defensa (conocido como *Blue Team*) o de ataque (conocido como *Red Team*) dentro de un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés).

Contenidos:

Tema 1. Introducción a la ética en la ciberseguridad

a. Importancia de la conducta humana en un ambiente laboral
b. Pensamiento ético subjetivo en la ciberseguridad

Tema 2. Consecuencias éticas y morales de los ataques cibernéticos

c. Prevención del mal uso de los datos informáticos
d. Resultados de buenas y malas prácticas en la ciberseguridad

Tema 3. Implementación práctica de los códigos de ética

e. Riesgos y la seguridad informática
f. Entendimiento de políticas, estándares y procedimientos

Tema 4. Interacción efectiva y ética para las relaciones laborales, profesionales y personales

g. Técnicas fundamentales para las relaciones interpersonales
h. Métodos para resolver conflictos
i. Destrezas de liderazgo

12. Programa de Cursos Libres de Inglés Conversacional.

Descripción del curso:

Este es el nivel 4 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso al igual que la gramática. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de fortalecer el nivel de competencia de Elementary A1.1+ según el MCERL.

Temática:

2. Man's Best Friends
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de preferencias en cuanto a mascotas.
    b. Reconocer vocabulario relacionado con mascotas.
    c. Utilizar adecuadamente la estructura: "What's It Like?" +/- adjective" en oraciones para describir mascotas.
    d. Aprender acerca del uso adecuado de los objetos directos e indirectos en oraciones.
    e. Utilizar adecuadamente modales tales como "should & could" para dar sugerencias de manera verbal o escrita.
    f. Aprender acerca del uso correcto de infinitivos y gerundios en oraciones y en preguntas simples.
    g. Comprender lecturas cortas acerca de animales y mascotas.
    h. Escribir un perfil corto acerca de animales.
3. Daily Life
    a. Hablar acerca de rutinas diarias utilizando el presente simple.
    b. Reconocer vocabulario relacionado con rutinas diarias.
    c. Utilizar adecuadamente la estructura del presente continuo en oraciones, preguntas cerradas y en preguntas abiertas (the -ing Form)
    d. Aprender acerca del uso adecuado de verbos modales (Can + Subject + Verb) para pedir ayuda y responder de forma oral y al escrita.
    e. Comprender lecturas cortas acerca de rutinas diarias de personas.

    f. Utilizar expresiones de frecuencia para completar un blog corto.
4. On Campus
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de temas académicos.
    b. Reconocer vocabulario relacionado con temas académicos.
    c. Aprender acerca del uso adecuado de “either” para estar de acuerdo y para dar opciones.
    d. Aprender acerca del uso correcto del pasado simple en oraciones y preguntas.
    e. Comprender lecturas cortas acerca de las clases del pasado y las clases en línea en el presente.
    f. Escribir un correo para dar consejos acerca de cómo obtener buenas notas en un examen.
5. Happy Times
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de celebraciones e invitaciones a actividades.
    b. Reconocer vocabulario relacionado con celebraciones y actividades.
    c. Aprender acerca del uso adecuado de expresiones utilizadas de manera formal para hacer invitaciones a fiestas y celebraciones.
    d. Aprender acerca del uso adecuado de la forma “Be Able To” para describir habilidad y capacidad para hacer algo o no.
    e. Aprender acerca del uso correcto de preposiciones de tiempo para utilizarlas de manera oral y escrita.
    f. Comprender lecturas cortas acerca de eventos deportivos mundiales.
    g. Escribir una invitación corta a un evento o celebración.
6. Making Money
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de trabajos y búsqueda de empleo.
    b. Reconocer vocabulario relacionado con trabajos y expresiones útiles para buscar empleo.
    c. Aprender acerca del uso adecuado de verbos compuestos (phrasal verbs) de forma oral o escrita.
    d. Aprender acerca del uso correcto de verbos causativos de forma oral y escrita.
    e. Comprender lecturas cortas acerca de trabajos.
    f. Escribir un perfil acerca de una hoja de vida.
7. On the Road
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de viajes.
    b. Reconocer vocabulario relacionado con viajes.
    c. Aprender acerca del uso de “yet” para describir su uso al referirse a una acción inmediata.
    d. Aprender acerca del uso adecuado de expresiones tales como “A few of + N vs. A few + N” de forma oral y escrita.

e. Aprender acerca del uso correcto del futuro (going to + verb) en oraciones, preguntas cerradas y en preguntas abiertas.
f. Comprender lecturas cortas acerca de viajes y destinos vacacionales.
g. Escribir un correo acerca de planes de viaje.

13. Ingeniería social.

Descripción del curso:

Este curso introduce conceptos importantes de la ingeniería social, entendida en ciberseguridad como una "estrategia no tecnológica que utilizan los atacantes cibernéticos, que depende en gran medida de la interacción humana y, a menudo, implica engañar a las personas para que rompan las prácticas de seguridad estándar".

En el mundo de hoy, la ingeniería social es reconocida como una de las formas más efectivas de obtener información y romper los muros de defensa. La seguridad de la información no sólo debe entenderse como un conjunto de elementos técnicos y físicos, sino como un proceso cultural de personas y organizaciones. En el campo de la seguridad a las personas se les conoce como el "eslabón más débil en su postura de seguridad" y es crítico aplicar controles que ayuden a disminuir el riesgo que éste pueda representar.

Las máquinas se construyen teniendo en cuenta la seguridad y se actualizan constantemente para corregir las vulnerabilidades, pero no se puede decir lo mismo de los humanos, quienes por naturaleza confían ya que la mente de los humanos está constantemente a la deriva y pensando en muchas cosas que no tienen nada que ver con la seguridad.

Según el perfil profesional, se desarrollarán las competencias que le permitan el estudio de conocimientos y habilidades sobre los principales conceptos de la ingeniería social tales como ataques y métodos, recolección de información, personalidad del atacante, víctimas típicas entre otros, así como el conocimiento del fraude, las vulnerabilidades que exponen a la organización, etc.

Contenidos:

Tema 1: Etapas de un ataque de ingeniería social

- Terminología básica de la ingeniería social
- Identificación de mecanismos relacionados al ataque de ingeniería social
- Análisis del perfil de su objetivo

Tema 2: Creación de ataques de ingeniería social

- Principios psicológicos utilizados en ingeniería social
- Recopilación de información de su objetivo
- Herramientas básicas de Ingeniería social

Tema 3: Defensas de ataques de ingeniería social

- Metodologías de defensa de ataques de ingeniería social
- Estudio de casos prácticos
- Contramedidas de la ingeniería social

14. Estándares de seguridad de la información.

Descripción del curso:

En este curso se propone la formación de los participantes en conocimientos y habilidades para el uso correcto de los diferentes estándares de seguridad.

El avance de la tecnología produjo varios dispositivos que se usan en la sociedad diariamente para interconectar el mundo. Esta creciente conectividad, sin embargo, produce mayor riesgo de robo, fraude y abuso en la infraestructura tecnológica. Hay una necesidad de establecer una política comprensiva de seguridad de la información dentro de todas las organizaciones.

Se necesita asegurar la confidencialidad, integridad y disponibilidad de la información corporativa vital y de la información del cliente o usuarios por medio de los estándares de

seguridad de la información para proteger los sistemas de red y todos los datos contra el uso no autorizado o los daños. A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización. A nivel del estado, la seguridad nacional, la seguridad y el bienestar de los ciudadanos están en juego.

Contenidos

Tema 1: Clasificación de datos

- Fundamentos de la clasificación de los datos
- Gobernanza
- Diferentes daños a la organización: económicos, técnicos, reputación

Tema 2. Análisis de estándares de seguridad de la información

- Requerimientos estándares de las normas ISO. 27001
- Instituto Nacional de Estándares y Tecnología (NIST)
- Objetivos de control para las Tecnologías de la Información (COBIT). Un marco para el gobierno y Gestión de las TI
- Biblioteca de infraestructura de Tecnología de la Información (ITIL)
- Tarjetas de pago (PCI/DSS)
- HIPAA

Tema 3. Políticas y procesos de aplicación

- Controles físicos
- Controles administrativos
- Controles lógicos

15. Programa de Cursos Libres de Inglés Conversacional.

Descripción del curso:

Este es el nivel 5 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso al igual que la gramática. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de guiar a los estudiantes de un nivel cero de conocimiento del idioma hacia un nivel de competencia de Beginner A1.1 según el MCERL.

Temática:

1. At the Department Store
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de cómo responder a preguntas relacionadas con ubicaciones y direcciones.
    b. Reconocer vocabulario relacionado con preposiciones y frases para hablar acerca de direcciones.
    c. Reconocer vocabulario simple acerca de ir de compras.
    d. Utilizar adecuadamente la estructura: “Where the things are [Where is/Where are?” en oraciones para ubicar lugares.
    e. Comprender conversaciones cortas y simples acerca del uso de las preposiciones de lugar y objetos que se pueden comprar en una tienda por departamento.

f. Aprender acerca del uso adecuado de los imperativos en oraciones simples.
g. Comprender una lectura corta acerca de ir de compras.
h. Escribir direcciones simples y completar oraciones utilizando un mapa como referencia.

2. Out in Nature
    a. Reconocer vocabulario y expresiones relacionadas con la naturaleza.
    b. Comprender conversaciones cortas y simples acerca de la naturaleza y el ambiente.
    c. Aprender acerca del uso adecuado del uso de la palabra “like” en diferentes contextos, así como de expresiones para esperar buenas noticias tales como “can’t wait (to + verb)” y “be looking forward to + v-ing” .
    d. Aprender acerca del uso adecuado de las conjunciones subordinadas en oraciones simples.
    e. Comprender una lectura corta acerca de algunas maravillas del mundo.
    f. Completar un perfil de un lugar turístico utilizando el vocabulario y las expresiones vistas en la unidad.
3. Food to Go
    a. Responder preguntas simples acerca de preferencias en alimentos y tipos de comidas.
    b. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de cómo responder a preguntas relacionadas con la compra de alimentos en distintos restaurantes.
    c. Reconocer vocabulario relacionado con palabras que se utilizan en un restaurante.
    d. Comprender conversaciones cortas y simples acerca del uso de las palabras que se utilizan al comer en algún restaurante o lugar de venta de comidas.
    e. Aprender acerca del uso adecuado de la expresión “just” y de expresiones que se utilizan para pedirle a una persona que espere.
    f. Aprender acerca del uso adecuado de los adjetivos en oraciones simples.
    g. Comprender una lectura corta acerca de comidas saludables y no saludables.
    h. Utilizar adjetivos de forma escrita para completar un perfil acerca de mi comida favorita.
4. Moving In
    a. Responder preguntas simples acerca de su lugar de residencia y los lugares aledaños.
    b. Reconocer vocabulario relacionado con palabras que se utilizan cuando se vive en un apartamento o casa.
    c. Comprender conversaciones cortas y simples acerca del uso de las palabras que se utilizan al hablar de la renta de un nuevo apartamento.
    d. Aprender acerca del uso adecuado de la estructure “would like + N” o “would like to + V” para dar sugerencias y hacer peticiones.

e. Aprender acerca del uso adecuado de los diversos tipos de adverbios en oraciones simples.
f. Comprender una lectura corta acerca de domicilios extravagantes y poco convencionales.
g. Utilizar un croquis de un domicilio para completar una conversación corta junto con la ayuda de un banco de palabras.

5. Time to Eat
    a. Responder preguntas simples acerca de hábitos alimenticios saludables.
    b. Reconocer vocabulario simple relacionado con tipos de comidas saludables.
    c. Comprender conversaciones cortas y simples acerca de comer saludablemente.
    d. Aprender acerca del uso en contexto de algunas expresiones y palabras.
    e. Aprender acerca del uso adecuado de expresiones para pedir comida, para hablar de hábitos alimenticios y frases para expresar certeza en oraciones simples.
    f. Aprender acerca de sustantivos contables y no-contables en oraciones simples y en diversos contextos.
    g. Comprender una lectura corta acerca de hábitos alimenticios saludables.
    h. Utilizar el vocabulario de la unidad para escribir acerca de una receta para una fecha especial.
6. Living with Technology
    a. Responder preguntas simples acerca del uso diario de la tecnología.
    b. Reconocer vocabulario relacionado con palabras relacionadas con tecnología y otros dispositivos electrónicos.
    c. Comprender conversaciones cortas y simples acerca del uso de la tecnología y sus aspectos positivos y negativos.
    d. Aprender acerca del uso adecuado de expresiones para dar sugerencias, hacer y responder a invitaciones y hablar acerca de preferencias con respecto a la tecnología.
    e. Aprender acerca del uso correcto del presente continuo en oraciones y preguntas simples.
    f. Comprender una lectura corta acerca del uso de una red social famosa.
    g. Utilizar una serie de acrónimos digitales y lenguaje tecnológico para completar de manera escrita una conversación corta.

16. Análisis de software malicioso.

Descripción del curso:
Este curso cubre la necesidad de formación de los futuros técnicos profesionales de la rama de la ciberseguridad, en el análisis del software malicioso y provee herramientas para el correcto análisis forense en el campo de la ciberseguridad, evitando poner en peligro sistemas informáticos.
Según el perfil profesional, el análisis del software malicioso (conocido también como *malware*) busca la identificación del alcance de los programas maliciosos y la creación de ambientes seguros de análisis para comprender las acciones resultantes de la ejecución de este software. Esto incluye conocimientos sobre el alcance de los daños dentro de una

organización por la ejecución de este tipo de programas; de técnicas de des ofuscación; investigación forense básica; recomendaciones técnicas para reducir el riesgo y las consecuencias de este tipo de software.

El curso busca formar analistas que puedan dar recomendaciones prácticas, correctas y fiables contra la ejecución de programa maligno en un ambiente informático, dominen el cómo establecer límites contra infecciones maliciosas y ejecuten análisis con herramientas especializadas para esta tarea. Se busca aplicar dichos conocimientos durante tareas ejecutadas por un equipo de defensa (conocido como *Blue Team*) dentro de un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés).

Contenidos:

Tema 1. Introducción a la clasificación de programas maliciosos
   a. Tipos de programas maliciosos y sus componentes
   b. Identificación de software malicioso por *hashes* y tipo de archivo

Tema 2. Arquitectura básica de un ataque informático
   a. Técnicas para obtener información sin ejecutar software malicioso
   b. Investigación OSINT contra software malicioso

Tema 3. Herramientas de análisis de programas maliciosos
   a. Anonimato web para el análisis de software malicioso
   b. Sistemas de captura *Honeypot*
   c. Encapsulamiento (*sandboxing*) y multi escaneo con software antivirus

Tema 4. Análisis forense básico contra software malicioso
   a. Entendimiento básico de técnicas de des ofuscación y depuración de software
   b. Análisis básico de software binario con programas desensambladores
      Introducción al análisis forense de memoria

17. Gestión de riegos empresariales.

Descripción del curso:

Este curso se enfoca en las metodologías, técnicas, procedimientos y prácticas para implementar un marco de trabajo enfocado en la gestión y análisis de riesgos de una organización, con el fin de minimizar el impacto de los posibles ataques a los sistemas de información. La información debe protegerse durante el envío, procesamiento y almacenamiento, mediante la implementación de diferentes mecanismos de seguridad. Sin embargo, a pesar de contar con sistemas de seguridad robustos, siempre existirán vectores de ataque y vulnerabilidades de las que se pueden aprovechar los atacantes. Es por ello que es de suma importancia contar con un plan que permita identificar los diferentes niveles de riesgos y categorizar correctamente las implicaciones ante un posible ataque y los costos que generaría a la organización.

Según el perfil profesional, se estudiaran conocimientos sobre el aseguramiento de la información, la matriz de riesgos y la gestión de riesgos, además se desarrollarán habilidades para la distinción de las distintas amenazas a las que se exponen los activos de una organización y parala utilización de herramientas para la creación de planes de gestión de riesgos y se fortalecerán las actitudes para tener responsabilidad por el cumplimiento de actividades relacionadas con la aplicación de estrategias y técnicas para la protección de las organizaciones y el trabajo en equipo.

Contenidos:

Tema 1. Aseguramiento de la información

   l. Identificación de amenazas
   m. Tipos de impacto y consecuencias de ataques
   n. Categorización de los niveles de riesgo

o. Riesgos cualitativos y cuantitativos

Tema 2. Matriz de riesgos

j. Definición de niveles de riesgo y su impacto
k. Escalas para definir los niveles de riesgo
l. Planeación y confección de una matriz de riesgos

Tema 3. Gestión de riesgos

l. Identificación de riesgos
m. Evaluación de riesgos
n. Controles y planes remediales
o. Procesos de revisión y trazabilidad

18. Programa de Cursos Libres de Inglés Conversacional.

Descripción del curso:
Este es el nivel 6 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de fortalecer el nivel de competencia lingüística Pre-Intermediate según el MCERL.

Temática:

1. Sonidos vocálicos
    a. Presentaciones de los articuladores en la producción de sonidos en inglés;
    b. Descripción de puntos de articulación de fonemas en inglés;
    c. Pronunciación de vocales: tense vowels vs. lax vowels, silent vowels.
    d. Word stress and vowel reduction
2. Acento
    a. Sentence stress and rhythm;
    b. Entonación y aspectos prosódicos en el habla: falling intonation and rising intonation;
    c. Thought groups;
    d. Linking vowel sounds;
    e. Phonological processes (sound deletion, assimilation, etc).
3. Identificación de sonidos
    a. Identificación de pares mínimos: minimal pairs;
    b. Identificación de letras mudas en inglés;
    c. Alfabeto fonético internacional (IPA).
4. Producción de sonidos
    a. Presentaciones orales;
    b. Producción escrita usando fonemas específicos;
    c. Conversaciones;
    d. Grabaciones.

19. Seguridad del software (OWASP).

Descripción del curso:
En el curso se estudiará el proyecto abierto Open Web Application Security Project (OWASP), creado en el 2001, que ofrece herramientas y recursos de seguridad gratuitos

para determinar y combatir las causas que hacen que el software sea inseguro y así ayudar a las organizaciones y profesionales de TI a a proteger las aplicaciones críticas y gestionar mejor el impacto emergente de los riesgos de seguridad de las aplicaciones. Ahora que las empresas utilizan cientos o miles de aplicaciones por día, a menudo implementadas sin la aprobación de los usuarios, es fundamental que los expertos en tecnología comprendan el panorama actual de riesgos y se preparen para enfrentar las amenazas emergentes.

El software inseguro está minando las infraestructuras críticas financieras, de salud, defensa, energía entre otras. Conforme el software incrementa su complejidad y capacidad de conectividad, la dificultad para alcanzar la seguridad en las aplicaciones se incrementa de manera exponencial. El veloz ritmo de los procesos modernos para el desarrollo del software, hacen que los riesgos más comunes sean esenciales de descubrir y resolver rápidamente de manera precisa. Ya no es permisible tolerar problemas de seguridad relativamente simples como los presentados en OWASP.

Según el perfil profesional, se desarrollarán las competencias que le permitan el estudio de conocimientos y habilidades sobre los principales conceptos del proyecto OWASP, convertido en estándar para seguridad en los programas y las aplicaciones, el análisis de los problemas y las recomendaciones.

Contenidos:

Tema 1. Introducción a la seguridad del software

- Principios del diseño de software seguro
- Conceptos generales sobre el desarrollo de aplicaciones web y móviles
- OWASP Top 10, CWE
- Revisión de Guía de desarrollo de OWASP
- Revision de Open Source Security Testing Methodology Manual (OSSTMM)

Tema 2: Análisis de vulnerabilidades del Top 10 de OWASP Web

- Inyección
- Pérdida de autenticación y gestión de sesiones
- Cross-Site Scripting (XSS)
- Control de acceso insuficiente
- Configuración de seguridad defectuosa
- Exposición de datos sensibles
- Control de acceso insuficiente
- Cross-Site Request Forgery (CSRF)
- Utilización de componentes con vulnerabilidades conocidas
- API desprotegidas

Tema 3: Análisis de vulnerabilidades dl OWASP Móviles

- Análisis de las principales vulnerabilidades relacionadas a las aplicaciones móviles y al OWASP Mobile Security Project
- Prácticas para la detección de vulnerabilidades
- Autenticación
- SQL injection
- XSS

20. Metodología y ciclo de vida de los ciberataques.

Descripción del curso:

En este curso se estudian los marcos teóricos de la ciberseguridad para ayudar a las personas que trabajan en el ámbito a identificar, detectar, aplicar y prevenir las ciber-amenazas persistentes, con metodologías tales como Cyber Kill Chain y las cinco fases del Ethical Hacking.

Acorde con el perfil profesional se desarrollará la capacidad para identificar la fase en que se encuentra un ataque, el alcance y riesgo del incidente, así como, predecir las siguientes acciones a tomar ante un atacante e implementar la mejor estrategia para detener las amenazas.
Se desarrollarán las habilidades en los participantes para que, a la hora de aplicar las estrategias de defensa, consideren los posibles puntos débiles, desde la red hasta la nube, así como las fortalezas y herramientas con las que se cuenta para lidiar con un ataque, pues en la mayoría de los ciberataques se aplican todas las fases de ataques, aunque pueden variar según el objetivo del atacante.

Contenidos:

Tema 1: Fases del *Hacking* ético

- Paso 1: Reconocimiento
- Paso 2: Escaneo
- Paso 3: Obtener el acceso
- Paso 4: Mantener el acceso
- Paso 5: Borrado de rastros/huellas

Tema 2: Metodología de Cyber Kill Chain

- Paso 1: Reconocimiento
- Paso 2: Preparación
- Paso 3: Distribución
- Paso 5: Instalación
- Paso 6: Comando y control
- Paso 7: Acciones sobre los objetivos

Tema 3: Prevención y mitigación

- Herramientas de prevención y mitigación
- Fortalecimiento de sistemas (*System hardening)*
- Estudios de casos reales

21. Programa de Cursos Libres de Inglés Conversacional.

Descripción del curso:

Este es el nivel 7 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso al igual que la gramática. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de fortalecer el nivel de competencia lingüística de Pre-Intermediate A.1.2 según el MCERL.

Temática:

1. Unidad 1: Shopping for Clothes
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de cómo describir la vestimenta que utilizan las personas.
    b. Comprender conversaciones cortas y simples acerca de descripciones de

ropa.
    c. Reconocer vocabulario relacionado con tallas de ropa, colores, materiales, etc.
    d. Comprender conversaciones cortas y simples acerca de personas comprando ropa para un evento social.
    e. Aprender acerca del uso en contexto de algunas expresiones y palabras.
    f. Aprender acerca de expresiones coloquiales, preguntas, respuestas y vocabulario relacionado a compra de artículos.
    g. Aprender acerca del uso adecuado de los adjetivos comparativos y superlativos en oraciones simples.
    h. Comprender una lectura corta de la moda juvenil.
    i. Escribir oraciones simples para describir un artículo de ropa utilizando el vocabulario aprendido en la unidad.
2. Unidad 2: Looking Good
    a. Reconocer expresiones cotidianas que se utilizan en conversaciones a nivel básico acerca de cómo describir la apariencia física de las personas.
    b. Comprender conversaciones cortas y simples acerca de descripciones de personas de acuerdo con sus características físicas.
    c. Reconocer adjetivos formales e informales para describir la apariencia de las personas.
    d. Comprender conversaciones cortas y simples acerca de personas describiendo brevemente la apariencia de algunos de sus familiares.
    e. Aprender acerca del uso en contexto de algunos antónimos, expresiones y palabras relacionadas con la unidad de estudio.
    f. Aprender acerca de expresiones coloquiales, preguntas, respuestas y vocabulario relacionado con países, nacionalidades y ocupaciones.
    g. Aprender acerca del uso adecuado del pasado simple en oraciones tanto positivas como negativas y en preguntas.
    h. Comprender una lectura corta relacionada con un método quirúrgico para cambiar la apariencia física.
    i. Escribir oraciones simples utilizando las estructuras de la unidad para describir una persona que trabaje como modelo para un comercial.
3. Unidad 3: A Helping Hand at Home
    a. Reconocer expresiones cotidianas y vocabulario que se utiliza en conversaciones a nivel básico acerca de objetos de uso cotidiano en casa.
    b. Comprender conversaciones cortas y simples acerca de aparatos de uso cotidiano en casa.
    c. Comprender conversaciones cortas y simples acerca de personas hablando acerca de algunos aparatos eléctricos de uso cotidiano en su lugar de residencia.
    d. Aprender acerca del uso en contexto de algunas expresiones y palabras relacionadas con la unidad de estudio.
    e. Aprender acerca de expresiones coloquiales, preguntas, respuestas y vocabulario relacionado con quejas durante el uso de aparatos eléctricos,

regatear al comprar electrodomésticos y describir el precio de dichos artículos.
    f. Aprender acerca del uso adecuado sustantivos y adjetivos posesivos y de conjunciones correlativas.
    g. Comprender una lectura corta acerca del uso idóneo y eficiente de algunos electrodomésticos para ahorrar energía.
    h. Escribir oraciones simples utilizando las estructuras de la unidad para describir un objeto eléctrico de uso cotidiano.
4. Unidad 4: Going Places
    a. Reconocer expresiones cotidianas y vocabulario que se utiliza en conversaciones a nivel básico acerca de medios de transporte de uso cotidiano.
    b. Comprender conversaciones cortas y simples acerca de medios de transporte que utilizan las personas.
    c. Comprender conversaciones cortas y simples acerca de personas hablando de lugares que se pueden frecuentar durante su estadía en un sitio vacacional.
    d. Aprender acerca de estructuras gramaticales, expresiones y vocabulario relacionado con dar y pedir direcciones.
    e. Aprender acerca del uso adecuado de verbos modales y de oraciones subordinadas.
    f. Comprender una lectura corta acerca de medios de transporte no tradicionales.
    g. Escribir oraciones simples para dar direcciones utilizando un mapa y el vocabulario de la unidad de estudio.
5. Unidad 5: Not Feeling So Good
    a. Reconocer expresiones cotidianas y vocabulario que se utiliza en conversaciones a nivel básico acerca de malestares y padecimientos de salud.
    b. Comprender conversaciones cortas y simples acerca de personas describiendo malestares y padecimientos que los aquejan.
    c. Comprender conversaciones cortas y simples acerca de una persona solicitando una cita médica para tratar un padecimiento.
    d. Aprender acerca de estructuras gramaticales, expresiones y vocabulario relacionado con agendar o solicitar una cita médica.
    e. Aprender acerca del uso adecuado de verbos copulativos y verbos causativos.
    f. Comprender una lectura corta acerca de tratamientos médicos naturales para combatir ciertos padecimientos y/o malestares.
    g. Escribir oraciones simples para contestar preguntas relacionadas al historial médico utilizando el vocabulario y las estructuras de la unidad de estudio.
6. Unidad 6: The Big Screen
    a. Reconocer expresiones cotidianas y vocabulario que se utiliza en

conversaciones a nivel básico acerca de tipos de películas.

b. Comprender conversaciones cortas y simples acerca de personas describiendo algunos tipos de películas.
c. Comprender conversaciones cortas y simples acerca de personas hablando acerca de una noche de películas en el cine.
d. Aprender acerca de estructuras gramaticales, expresiones y vocabulario relacionado con pedir disculpas, hablar acerca de expresiones de tiempo y discutir acerca de películas.
e. Aprender acerca del uso adecuado de expresiones de tiempo utilizando preposiciones en preguntas y oraciones; y también dar la hora en inglés.
f. Comprender una lectura corta acerca de algunos roles inusuales que han desempeñado algunos animales en algunas películas famosas durante la historia cinematográfica.
g. Escribir un párrafo corto acerca de una reseña de una película de gusto personal.

22. Laboratorio y herramientas para ciberataques:

Descripción del curso:

Con la digitalización del trabajo, automatización de procesos e interconexión a nivel mundial, el internet se ha convertido en un espacio de libre tránsito para los atacantes, que buscan constantemente obtener información, acceso a recursos, secuestrar infraestructura y datos para posteriormente pedir una recompensa o generar un daño económico, de disponibilidad o de reputación al afectado.

Acorde con el perfil profesional se estudiarán las herramientas tanto ofensivas como defensivas, obligación para cualquier especialista en el área de la ciberseguridad, permitiéndole generar estrategias para proteger la información y arquitectura de la organización, reaccionar ante un posible ataque de forma eficiente y elaborar planes de mejora basado en las lecciones aprendidas posterior al incidente.

Se desarrollarán las habilidades en los participantes de instalar y administrar herramientas ofensivas y defensivas, entendiendo que son y como encontrar vulnerabilidades en la organización, al igual que como ejecutar de forma satisfactoria un proceso de respuesta de incidentes.

Contenidos:

Tema 1: Herramientas para utilizar en cada etapa del proceso de un ataque.

- Herramientas para utilizar en la etapa de reconocimiento.
- Herramientas para utilizar en la etapa de enumeración
- Herramientas para utilizar en la etapa de ataque
- Proceso de documentación de los resultados

Tema 2: Herramientas para la protección de la infraestructura de una organización.

- Soluciones de encriptación, soluciones contra programas maliciosos, administración de equipos y contraseñas
- Soluciones web de diagnóstico, evaluación de reputación y uso de “Frameworks” de industria
- Uso de Redes Virtuales Privadas

Tema 3: Principales herramientas utilizadas por el equipo rojo y azul.

- Escáneres de vulnerabilidades
- Escáneres de puertos
- Analizadores de protocolos
- Metasploit y Armitage

Tema 4: Desarrollo de laboratorio final.

- Implementación de las principales herramientas de seguridad ofensiva y defensiva.
- Completar el proceso de reconocimiento y recolección de datos del entorno.
- Realizar ejercicios de vulnerabilización de la red y los servicios ofrecidos por una organización.
- Enumerar los hallazgos y las vulnerabilidades detectadas en el entorno usando "mainframes" de industria.
- Desarrollar una bitácora con lecciones aprendidas y acciones por tomar para mejorar la superficie de riego de la organización, priorizando de manera correcta las acciones más urgentes.

23. Informática forense.

Descripción del curso:

El curso Informática forense busca formar a los estudiantes en el área investigativa y analítica de la ciberseguridad. Dicha área, ha crecido en los últimos años debido al incremento exponencial de los crímenes informáticos.

La informática forense, a diferencia de otras áreas de la ciberseguridad no busca prevenir ni defender un sistema, sino más bien identificar, recolectar, categorizar evidencia de un sistema informático, una computadora o toda una red de ellas. Este conjunto de técnicas y prácticas buscan recoger toda la información necesaria, para realizar un reporte que se puede sostener como evidencia ante una corte de ley para incriminar a los atacantes.

Partiendo de estas bases, el curso ofrece un espacio de aprendizaje donde se nivela, expande y formaliza contenidos para investigar sistemas operativos, técnicas de investigación de software, redes y sistemas operativos además de un conjunto de herramientas básicas y de licencia libre para realizar un análisis y el reporte forense.

Según el perfil profesional, se desarrollarán competencias y habilidades que permitan al estudiante el estudio y adquisición de conocimientos para que junto con las herramientas pueda analizar un caso, recabar información, realizar una línea del tiempo y colocarla en forma de un reporte en función de un Análisis Forense junto con ejercicios de investigación.

Contenidos:

Tema 1: Fundamentos de informática forense

- •Concepto de cómputo forense
- •Los delitos tecnológicos y las nuevas tendencias
- •El cibercrimen
- •La evidencia digital
- •Identificación y Preservación de Evidencia Digital
- •Análisis y Presentación de Resultados

Tema 2: Identificación

- •Herramientas para adquisición
- •Cadena de Custodia
- •Fuentes de evidencia
- •Inventario de evidencia y plan de adquisiciones

Tema 3: Preservación

- •Sistemas de protección contra escritura por hardware y software
- •Adquirir imágenes forenses
- •Imágenes lógicas, memoria volátil y sistemas operativos en vivo
- •Verificación con algoritmos HASH

Unidad 4: Análisis y presentación de la Evidencia

- •Sistemas FAT, NTFS
- •Sistemas EXT, HFS y APFS

•Registros: SAM, Software
•Logs de un Sistema Windows
•Most recently use, MRU) y Shellbags
•Bandejas de reciclaje
- Arranque y ejecución de procesos en sistemas operativos
- Archivos de autenticación
- Análisis temporal del sistema
- Presentación del informe ante autoridades judiciales

24. Programa de Cursos Libres de Inglés Conversacional.

Descripción del curso:
Este es el nivel 8 de una secuencia de trece cursos teóricos-prácticos más un último nivel práctico enfocado en la expresión oral. Este nivel le permitirá a la persona usuaria iniciar sus conocimientos del idioma inglés. El curso está planeado en virtud de que la persona usuaria desarrolle la competencia lingüística requerida para comunicarse en inglés de acuerdo con situaciones cotidianas. Este curso integra las cuatro habilidades básicas del idioma: lectura, escritura, comprensión auditiva y producción oral; no obstante, tiene un énfasis en desarrollar la comprensión auditiva y la conversación. La lectura y la escritura son complementos del objetivo general del curso al igual que la gramática. En cuanto a la teoría, se presentan funciones de lenguaje y de vocabulario, así como estrategias de autocorrección con el fin de fortalecer el nivel de competencia lingüística Pre-Intermediate A2 según el MCERL.
Temática:
1. Unit 1: How Do You Feel
    a. Vocabulario acerca de sentimientos positivos y negativos.
    b. Preguntar oralmente y por escrito acerca de los sentimientos de otra persona.
    c. Expresar oralmente y por escrito sentimientos con otras personas.
    d. Hablar, escuchar y escribir acerca de dar y recibir buenas y malas noticias.
    e. Comprender audios acerca de emociones y sentimientos en diferentes situaciones cotidianas.
    f. Uso de los adjetivos con terminación ING o ED.
    g. Uso de adjetivos con preposiciones.
    h. Comprender textos relacionados a los sentimientos de los animales.
    i. Demostrar entendimiento de un texto y escribir historias utilizando el vocabulario relacionado a sentimientos.
2. Unit 2: All in Good Fun
    a. Vocabulario de actividades en tiempo libre.
    b. Preguntar y dar opiniones oralmente y por escrito.
    c. Expresar oralmente lo que nos gusta y nos disgusta.
    d. Hacer planes para salir a disfrutar del tiempo libre.
    e. Comprender audios acerca de los planes de diferentes personas.
    f. Utilizar frases en contexto para expresar lo que nos gusta y disgusta.
    g. Uso de gerundios e infinitivos
    h. Comprender textos acerca las actividades extremas que algunas personas practican.
    i. Escribir e-mails invitando a un amigo a disfrutar del tiempo libre el fin de semana.
    j. Expresar por escrito mis actividades favoritas.
3. Unit 3: Game Time
    a. Vocabulario relacionado a deportes populares en diferentes partes del

mundo.
   b. Utilizar frases en contexto con los verbos adecuados de los diferentes deportes.
   c. Hablar de lesiones.
   d. Expresar oralmente y por escrito requisitos para practicar un deporte.
   e. Conversar acerca de deporte en general.
   f. Comprender audios acerca de personas que practican deportes y/o se lesionan.
   g. Utilizar frases en contexto para explicar o solicitar los requisitos que se necesitan para practicar un deporte.
   h. Uso de los verbos modales.
   i. Sinónimos
   j. Utilizar correctamente en contexto el tiempo pasado continuo.
   k. Entender un texto acerca un caso de la vida real de una deportista.
   l. Demostrar entendimiento de la biografía de un futbolista famoso y completar una entrevista a un compañero acerca de sus gustos y preferencias acerca del deporte.
4. Unit 4: Rain or Shine
   a. Vocabulario relacionado a condiciones climáticas.
   b. Vocabulario relacionado a implementos necesarios para afrontar condiciones climáticas.
   c. Preguntar oralmente y por escrito acerca las diferentes estaciones del año y estado del tiempo.
   d. Describir condiciones del tiempo y preguntar acerca de ellas.
   e. Expresar oralmente mis planes.
   f. Identificar información específica en audios acerca de las condiciones del tiempo y estaciones.
   g. Utilizar correctamente en contexto el tiempo futuro simple con be+going to y will.
   h. Utilizar frases en contexto en futuro simple.
   i. Comprender textos acerca de cómo el clima influye en la construcción de una casa o edificio.
   j. Escribir reportes del clima utilizando la gramática y vocabulario aprendido en la unidad.
5. Unit 5: Eating Out
   a. Vocabulario relacionado a los diferentes tipos de comidas.
   b. Vocabulario relacionado a restaurantes.
   c. Expresar oralmente y por escrito mis preferencias alimenticias
   d. Hacer planes y recomendaciones para salir a comer con alguna persona.
   e. Utilizar freses en contexto para ordenar en un restaurante y solicitar algo en especial.
   f. Comprender audios acerca de comidas y menús.
   g. Utilizar correctamente los pronombres indefinidos
   h. Comprender textos acerca de la variedad culinaria mundial.
   i. Demostrar entendimiento de un texto y escribir historias utilizando el vocabulario relacionado a sentimientos.
   j. Escribir un reporte acerca de alguna experiencia en su restaurant favorito.
6. Unit 6: School Life
   a. Vocabulario relacionado a rasgos de personalidad.
   b. Utilizar frases en contexto para expresar mi personalidad.
   c. Discutir problemas personales y mis planes a futuro.

d. Definir mis metas personales.
e. Identificar palabras clave en audios relacionados a la personalidad.
f. Uso correcto del condicional cero y uno.
g. Uso correcto de sustantivos y verbos.
h. Comprender textos de personas que disfrutan de experimentar intercambios para hacer voluntariados.
i. Completar una fórmula para optar por un intercambio.

25. Práctica profesional.

Descripción del curso:
Este curso representa la fase final del técnico en Ciberseguridad, donde los estudiantes pondrán en marcha los conocimientos adquiridos durante todo el proceso de enseñanza-aprendizaje.
Se pretende implementar de manera integral las competencias establecidas en el Estándar de Cualificación de Ciberseguridad establecido por el Marco Nacional de Cualificaciones (CE1, CE2, CE3 y CE4). Asimismo, se consolida la perspectiva multi y transdisciplinaria la cual insta a los estudiantes a que relacionen a un nivel profundo los conocimientos de la Seguridad Informática, compromiso profesional y ético con la organización en la que se desempeñarán.
El estudiante deberá brindar su mayor esfuerzo y conocimiento en procura de alcanzar los objetivos planteados en el curso, el cual está enfocado en el cierre del proceso que culmina con la presentación de un informe de práctica.
El papel del docente será en todo momento de facilitador y guía del proceso de la práctica profesional, permitiendo la construcción y autorregulación de los aprendizajes. Para todos los fines académicos, el curso de la Práctica contará con un profesor titular a cargo del curso que acompañará a los estudiantes en sus labores de campo y sistematización de la información.
Según el perfil profesional, se integran los conocimientos, habilidades y actitudes desarrolladas a lo largo del técnico, mediante la aplicación de herramientas relacionadas a la programación, los sistemas operativos, las normas y políticas de seguridad informática, para la resolución de situaciones en las organizaciones.
Contenidos:
Contenidos del Seminario de Ciberseguridad

Unidad 1. Elementos que conforman el proceso multidisciplinario y transdisciplinario de la Ciberseguridad

- -Herramientas de Ciberseguridad como medio para generar valor.
- -Herramientas de mejora de procesos para la Ciberseguridad.
- -Herramientas de gestión de proyectos de Ciberseguridad.

Unidad 2. Tendencias y enfoques globales de la Ciberseguridad y los principios éticos

- -Transformación digital y Ciberseguridad
- -Principios éticos aplicados a la práctica profesional en Ciberseguridad.

Unidad 3. Diseño de Informe de práctica supervisada en Ciberseguridad.

- -Introducción
- -Desarrollo
- -Conclusiones

Unidad 4. Diseño preliminar del plan de trabajo

- -Informe de progreso del plan de trabajo
- -Plan de Trabajo Final

Contenidos de la Práctica Supervisada en Ciberseguridad

Unidad 1: Logical Framework de la Práctica en Ciberseguridad (2 semanas)

- -Aspectos conceptuales de una práctica
- -Organización y preparación de la Práctica.
- -Roles y responsabilidades del supervisor y del practicante.
- -Los permisos necesarios para realizar las prácticas profesionales en una empresa.
- -La importancia del diagnóstico en Ciberseguridad.

Unidad 2: Observación y Desarrollo del Diagnóstico en Ciberseguridad por parte del Practicante 2 semanas (60 horas)

En esta fase el practicante entra en contacto directo con los encargados de la organización con el grupo ya sea de ingenieros o informáticos encargados de la seguridad informática.

El practicante deberá recopilar la información para elaborar el diagnóstico de la organización que tendrá a su cargo. En este periodo de observación es de vital importancia que el practicante permanezca en la organización durante la práctica (4 por semana).

Para que el periodo de la observación sea provechoso, el practicante deberá:

- -Identificar las áreas de la organización relacionadas a Ciberseguridad
- -Observar y participar en actividades productivas que realice la organización durante este período.
- -Consultar la bibliografía que emplea el ingeniero en Ciberseguridad tales como: libros de apoyo, de consulta, materiales y otros disponibles.
- -Observar atentamente las diferentes actividades relacionadas a la Ciberseguridad.
- Las tareas que debe realizar el practicante para desarrollar el diagnóstico en Ciberseguridad son:
- -Diseñar objetivos, propósitos, problemas o categorías de análisis que guiaran el diagnostico en cada ámbito de la seguridad informática.
- -Diseñar y aplicar las técnicas e instrumentos para recoger la información de las actividades de la organización
- -Recolectar los datos.
- -Sistematización, análisis e interpretación de los datos.
- -Edición de los datos en información para la toma de decisiones.
- -Desarrollo del informe final (Introducción, objetivos, análisis de datos, visualización de los datos, conclusiones, anexos y bibliografía).

Unidad 3: Planeamiento Empresarial (2 semanas)

-Asesoramiento a la empresa: la persona estudiante se reunirá, mediante la plataforma *teams*, con su supervisor(a) de práctica y entregará el plan o la estrategia de Ciberseguridad por tema a tratar con los encargados de la organización.

-Retroalimentación del supervisor: el supervisor, deberá revisar el plan y devolverlo para realizar las correspondientes correcciones y recomendaciones, las cuales deberán efectuarse para una segunda revisión. Cuando el borrador del plan tenga el visto bueno, deberá prepararse la edición final y entregar una copia digital de éste al docente de la escuela, antes de que el practicante inicie la primera lección con el grupo de niños.

Unidad 4: Práctica Intensiva (2 semanas) 72 horas

Aspecto 1: El practicante debe demostrar responsabilidad y capacidad suficiente para resolver los problemas asignados relacionados a la Ciberseguridad.
Aspecto 2: El practicante debe demostrar independencia, habilidad para adaptar la acción de mejora de modo que responda a los intereses y los objetivos de la organización y que sepa aprovechar los recursos que se le ofrecen para facilitar y favorecer los procesos productivos. De manera específica, se le exigirá la presentación de las ideas innovadora para la mejora continua del proceso.
Aspecto 3: en la primera visita de práctica, el supervisor aplicará la evaluación del desempeño.
Aspecto 4: Durante las visitas el practicante deberá mantener la disciplina de manera que se pueda desarrollar la mejora en forma adecuada y provechosa.
Aspecto 5: Se deben aplicar diversos métodos y técnicas para resolver problemas, considerando la Política de la empresa vigente.
Aspecto 6: Todos los planes se deberán llevar siempre juntos en un portafolio digital de Ciberseguridad que garantice el orden y la visualización, para que, tanto el practicante, el supervisor y los encargados de la empresa puedan, en el momento oportuno, observar la integración de todo el proceso.
Aspecto 7: Los planes de mejora, deberán ser sometidos a consideración tanto de los encargados de la organización como del supervisor.
Aspecto 8: Presentar con 8 días de anticipación los planes de mejora por área, materiales, resúmenes, instrumentos de medición, evaluación y otros, al supervisor para su revisión y aprobación.
Aspecto 9: Es deber del practicante presentarse a la organización con su respectivo plan de mejora, el cual deberá entregarlo al supervisor al momento de la observación.
Aspecto 10: El practicante debe asistir a tutorías (atención individual) con el supervisor de la práctica. En este espacio se revisarán planes, materiales, mediciones, y otros. A la vez se comentará las acciones a evaluar. El supervisor agendará las reuniones por *Microsoft Teams* o ZOOM en común acuerdo con cada estudiante. La asistencia del estudiante es obligatoria.
Aspecto 11: Si los encargados de la organización solicita el retiro del practicante por problemas en el dominio de los conocimientos, control y orden de los procesos, u otros que de su función se deriven, éste perderá automáticamente el curso.

ANEXO C

PERFIL DEL DOCENTE



CONSEJO NACIONAL DE RECTORES
OFICINA DE PLANIFICACIÓN DE LA EDUCACIÓN SUPERIOR

DC-03 Perfil de la persona docente | Versión 02

Aprobado por:
Fecha de implementación: | Copia N°. 01



Perfil de la persona docente que se requiere para impartir cada uno de los cursos o módulos.

Técnico		
Nombre del técnico	**Ciberseguridad**	
Nivel del técnico	**Técnico 3**	
Código del estándar	**0612-14-03-3**	
Curso/módulo que impartirá el docente		
Certificaciones específicas requeridas para impartir el curso/módulo	No aplica	Si aplica, específique:

Estudios requeridos	
Grado académico mínimo requerido:	Carrera
Bachiller Universitario	Ingeniería en informática, computación, ingeniería en sistemas, sistemas de Información, sistemas WEB tecnologías de la información, auditoría de tecnologías y sistemas de información, análisis de datos, telemática, ciberseguridad, análisis de sistemas, bases de datos, servidores web libres, programación, ingeniería de software. Otra carrera atinente al curso por impartir.

Experiencia laboral requerida	
Rango de años requerido	Puestos relacionados con el curso/módulo del técnico
1 año en adelante	Un año de experiencia profesional en una organización o institución, desempeñándose alguno de los siguientes temas: redes, ciberseguridad, telemática, programación, sistemas operativos, seguridad de la información, auditoría de TI.

Experiencia docente requerida	
Rango de años requerido	Cursos en la carrera docente relacionados con el curso/módulo del técnico
6 meses	Impartiendo lecciones en temas de redes, ciberseguridad, telemática, programación, sistemas operativos, seguridad de la información, auditoría de TI.

CONSEJO NACIONAL DE RECTORES

UCR

TEC

UNA

UNED

UTN Universidad Técnica Nacional

/Consejo Nacional de Rectores www.conare.ac.cr 2519-5700

1.3 km. norte de la Embajada de los Estados Unidos. Pavas, San José, Costa Rica