MARCO NACIONAL DE CUALIFICACIONES
EDUCACIÓN Y FORMACIÓN TÉCNICA PROFESIONAL
COSTA RICA

Catálogo Nacional de Cualificaciones de la Educación y Formación Técnica Profesional de Costa Rica

FR MNC 03
EDICIÓN 02
Aprobado
12/08/2019

Estándar de Cualificación

Ciberseguridad

Código 0612-14-03-4-01

Versión 01

Junio, 2020

EMPEZAR

Índice

EL MARCO NACIONAL DE CUALIFICACIONES DE LA EDUCACIÓN Y FORMACIÓN TÉCNICA PROFESIONAL DE COSTA RICA

Aprobación

El Marco Nacional de Cualificaciones de la Educación y Formación Técnica Profesional de Costa Rica (MNC-EFTP-CR) fue aprobado en la sesión N° 37- 2016, celebrada por el Consejo Superior de Educación el día 18 de julio del 2016, mediante acuerdo N° 06-37-2016 y actualizado en el acuerdo N° 04-60-2019, según consta en el Decreto Ejecutivo N° 39851-MEP-MTSS, el cual fue publicado el martes 6 de setiembre del 2016 en el Alcance N° 161A de la Gaceta.

En cuanto a su definición, propósito general y componentes, el documento del MNC-EFTP-CR (2019), en su Capítulo III, establece:

- Definición

El Marco Nacional de Cualificaciones de Educación y Formación Técnica Profesional de Costa Rica (MNC-EFTP-CR) es la estructura reconocida nacionalmente, que norma las cualificaciones y las competencias asociadas a partir de un conjunto de criterios técnicos contenidos en los descriptores, con el fin de guiar la formación; clasificar las ocupaciones y puestos para empleo; y facilitar la movilidad de las personas en los diferentes niveles; todo lo anterior de acuerdo con la dinámica del mercado laboral (p.51).

- Propósito general

El MNC-EFTP-CR norma el subsistema de educación y formación técnica profesional, a través de la estandarización de los niveles de formación, descriptores, duración y perfiles de ingreso y egreso de la formación, entre otros. Establece la articulación vertical y horizontal en el sistema educativo costarricense y orienta la atención de la demanda laboral. Además, asocia las cualificaciones con campos de la educación establecidos en la Clasificación Internacional Normalizada de la Educación (CINE-F-2013) y la normativa salarial (p.50).

- Componentes

El MNC-EFTP-CR establece un sistema de nomenclatura de cinco niveles de técnico. Cada nivel de cualificación cuenta con su respectivo descriptor, requisito mínimo de escolaridad para el ingreso, rango de duración del plan de estudios y requisito mínimo de escolaridad para la titulación (p.52).

Con respecto a los Estándares de cualificación y al Catálogo Nacional de Cualificaciones (CNC) el MNC-EFTP-CR, establece:

> Los estándares pueden entenderse como definiciones de lo que una persona debe saber, hacer, ser y convivir para ser considerado competente en un nivel de cualificación. Los estándares describen lo que se debe lograr como resultado del aprendizaje de calidad.
>
> El estándar de cualificación es un documento de carácter oficial aplicable en toda la República de Costa Rica, establece los lineamientos para la formulación y alineación de los planes de estudios y programas de la EFTP, que se desarrollan en las organizaciones educativas.
>
> El Catálogo Nacional de Cualificaciones (CNC) asume la organización por campos de la educación que establece la CINE-F-2013, agregando el Campo de la Oferta Educativa y se subdivide en Campo Profesión y el Campo Cualificación reconocida a nivel nacional e internacional, las cuales son asociadas al Clasificador de Ocupaciones de Costa Rica (COCR) u otros.
>
> La metodología incorpora la Clasificación Internacional Normalizada de la Educación (CINE-F-2013)1 con el objetivo de codificar las cualificaciones para el Catálogo Nacional de Cualificaciones de EFTP, normalizar la oferta educativa y los indicadores de la estadística de la EFTP en el ámbito nacional e internacional.

El Campo Detallado

Según Clasificación Internacional Normalizada de la Educación, Campos de la Educación y la Formación 2013 (CINE-F 2013) – Descripción de los campos detallados, el campo detallado 0612 Diseño y administración de redes y bases de datos, incluye:

Diseño y administración de redes y bases de datos es el estudio del diseño, mantenimiento e integración de aplicaciones de software. Se incluyen aplicaciones de medios informáticos.

Los programas y certificaciones con los siguientes contenidos principales se clasifican aquí:

- Gestión y administración de computadores
- Aplicaciones de medios informáticos
- Instalación y mantenimiento de redes informáticas
- Estudios de administradores de bases de datos

- Administración de tecnología de información
- Seguridad en tecnología informática
- Administración de red
- Diseño de redes
- Diseño web (p.25)

Créditos

Elaboración

- Personas que representan a las organizaciones, instituciones y empresas que participaron en la elaboración del Estándar de Cualificación[1]

Carlos Argüello Bojorge, ISESA
Hans Lothar Lara, INA
Heidy Cordonero Solano, MEP
José Pablo Calvo Suárez, UNA
Josué Rodríguez Vargas, VLA
Josué Segnini Salas, USJ
Katia Mauricio Vásquez, UNA

- Personas que representan a las organizaciones, instituciones y empresas que participaron en la validación del Estándar de Cualificación:

Departamento de Investigación Aplicada, Monitoreo y Evaluación, CINDE
Esteban Jiménez Cabezas, ATTICYBER
Hernando Segura Bolaños, Cyberlabs
Jeff Cascante Rosales, Fortinet
José Pablo Esquivel Escalante, CISCO-NetAcad
Kenneth Monge Quirós, Poder Judicial
Óscar Ramírez Rodríguez, CISCO
Roberto Mata Medina, Organismo de Investigación Judicial

[1] Se anexa el listado de organizaciones, instituciones y empresas, informante clave, durante el proceso de elaboración del Estándar de Cualificación.

- Personas que representan la Instancia de Gestión y Registro de Estándares de Cualificación que asesoraron durante el proceso:

  Lourdes Castro Campos.

Acuerdo de aprobación oficial

El presente Estándar de Cualificación fue aprobado por la Comisión Interinstitucional para la Implementación y Seguimiento del Marco Nacional de Cualificaciones de la Educación y Formación Técnica Profesional de Costa Rica, mediante el Acuerdo N° 03-02-2020, el día diez del mes junio del año dos mil veinte.

I. Identificación de la cualificación

1

Codificación Cualificación: 0612-14-03-4-01

2

Cualificación (Nombre): Ciberseguridad

3

Nivel de cualificación: Técnico 4

4	5
Campo Amplio: 06 Tecnologías de la información y la comunicación (TIC)	**Campo Específico:** 061 Tecnologías de la información y la comunicación (TIC
6	7
Campo Detallado: 0612 Diseño y administración de redes y bases de datos	**Campo Profesión:** 14 Diseño y Administración de Redes y Bases de Datos
8	9
Campo Cualificación: 03 Ciberseguridad	**Tiempo de Vigencia del Estándar de Cualificación:** 5 años
10	11
Fecha de actualización: junio, 2025	**Nivel de escolaridad requerido para el ingreso:** III Ciclo Educación General Básica

12

Nivel de escolaridad requerido para titulación: Bachillerato en Educación Media

13

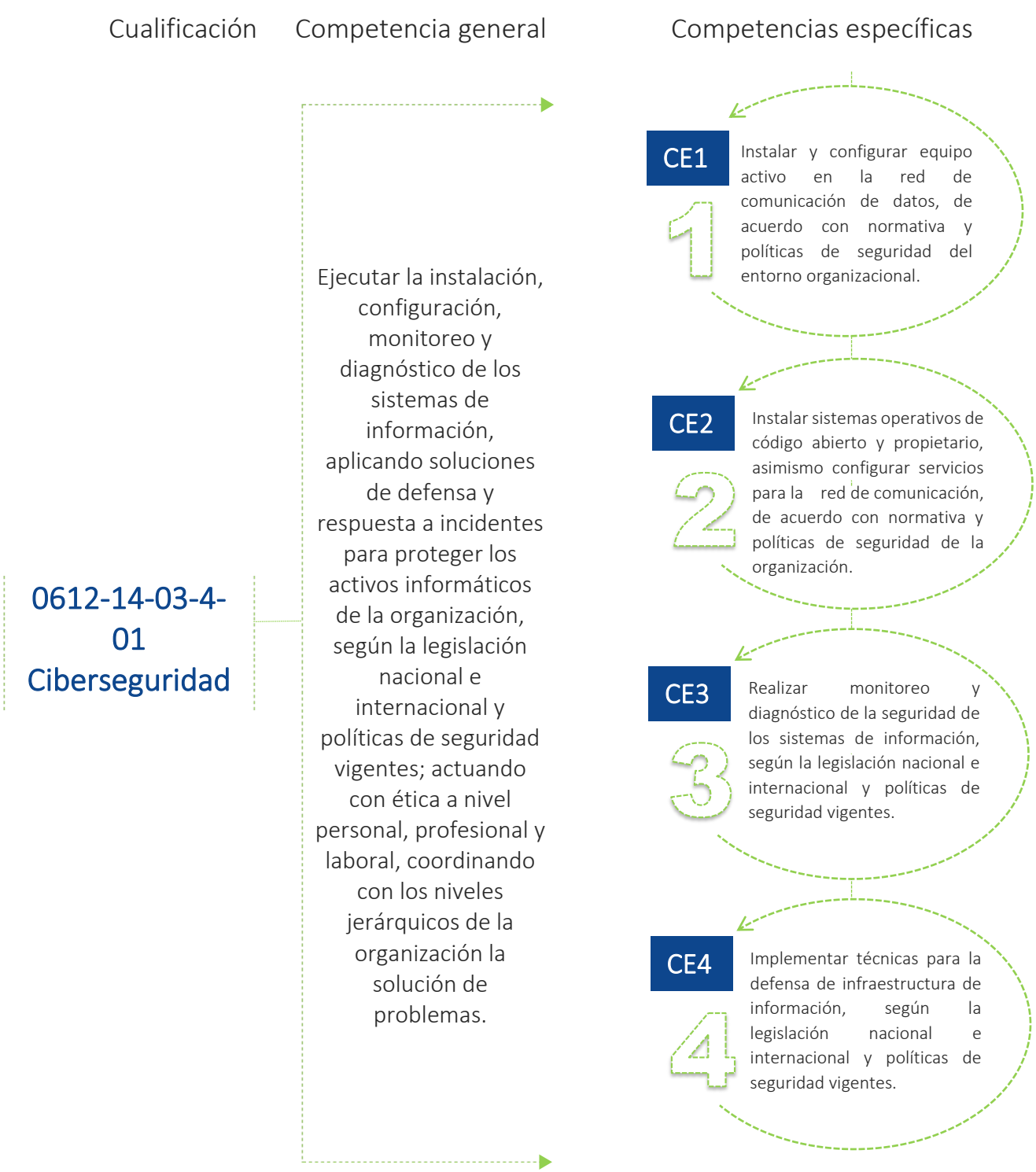
Competencia general: Ejecutar la instalación, configuración, monitoreo y diagnóstico de los sistemas de información, aplicando soluciones de defensa y respuesta a incidentes para proteger los activos informáticos de la organización, según la legislación nacional e internacional y políticas de seguridad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

14

Competencias específicas de otros estándares de cualificación requeridas para titulación de este: No aplica

15

Mapa de cualificación:



II. Descripción de las competencias específicas

Competencias específicas (CE)	Resultados de aprendizaje[2]
	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.

Evaluación del logro de la competencia específica N°1

Evidencias CE1

Conocimientos:

- Normativa y políticas de seguridad del entorno organizacional.
- Normas de aseguramiento de la calidad establecidas a nivel nacional e internacional.

Desempeño:

- Instala y configura equipo activo en la red de comunicación.
- Diagnostica y corrige fallas en equipo activo.

[2] Resultados de aprendizaje según elementos del descriptor. Aplicación y saberes disciplinarios.

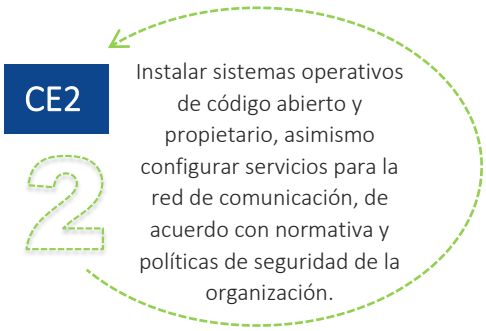
Nota: Los desempeños los realiza, según la legislación nacional e internacional y políticas de seguridad vigentes; actuando con ética a nivel personal, profesional y laboral, coordinando con los niveles

Producto: >

- Red de comunicación en estado óptimo de funcionamiento.
- Falla corregida en equipo activo.

Nota: Los productos los realiza, de acuerdo con normativa y políticas de seguridad del entorno organizacional.

Competencias específicas (CE)



Resultados de aprendizaje

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.

Evaluación del logro de la competencia específica N°2

Evidencias CE2

Conocimientos:

- Normativa y políticas de seguridad organizacionales.
- Normas de aseguramiento de la calidad establecidas a nivel nacional e internacional.

Desempeño:

- Instala y configura sistemas operativos de red de código abierto y propietario.
- Instala y configura los servicios para la red de comunicación en sistemas operativos de código abierto y propietario.

- Diagnostica y corrige fallas en sistemas operativos de red de código abierto y propietario.
- Diagnostica y corrige fallas los servicios para la red de comunicación en sistemas operativos de código abierto y propietario.

Nota: Los desempeños los realiza, 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.

Producto: >

- Sistema operativo de red de código abierto y propietario instalado y en funcionamiento.
- Servicio de red de comunicación en sistemas operativos de código abierto y propietario en funcionamiento.
- Falla corregida en sistema operativo de red de código abierto y propietario.
- Falla corregida en servicios de red de comunicación en sistemas operativos de código abierto y propietario.

Nota: Los productos los realiza, de acuerdo con normativa y políticas de seguridad de la organización.

Competencias específicas (CE)	Resultados de aprendizaje
	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.

Evaluación del logro de la competencia específica N°3

Evidencias CE3

Conocimientos:

- Legislación nacional e internacional en el campo de la seguridad informática.

Desempeño:

- Diagnostica anomalías y vulnerabilidades, mediante el monitoreo de tráfico de la red.

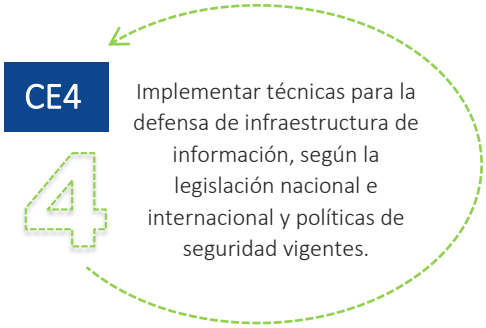
Nota: Los desempeños los realiza, según la legislación nacional e internacional y políticas de seguridad vigentes; actuando con ética a nivel personal, profesional y laboral, coordinando con los niveles jerárquicos de la organización la solución de problemas.

Producto:

- Informe de la configuración segura de la red.

Nota: Los productos los realiza, según la legislación nacional e internacional y políticas de seguridad vigentes.

Competencias específicas (CE)



Resultados de aprendizaje

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.

Evaluación del logro de la competencia específica N°4

Evidencias CE4

Conocimientos:

- Legislación en Ciberseguridad vigente.

Desempeño:

- Aplica técnicas para la defensa de infraestructuras de información.

Nota: Los desempeños los realiza, 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.

Producto: >

- Plan remedial para corrección de situaciones de vulnerabilidad.

Nota: Los productos los realiza, según la legislación nacional e internacional y políticas de seguridad vigentes.

III. Resultados de aprendizaje transversales a todas las competencias específicas[3]

• Aplica las normas de salud ocupacional, según protocolos establecidos por la organización.

• Desarrolla acciones relacionadas con la normativa ambiental.

• Trabaja en equipo de manera responsable, con orden y ética profesional.

• Aplica principios de servicio al cliente interno y externo.

• Aplica normas nacionales e internacionales para aseguramiento de la calidad.

• Coordina acciones y equipos de trabajo de manera asertiva.

• Propone soluciones creativas e innovadoras a proceso específicos.

• Plantea alternativas para la resolución de casos en el contexto laboral.

En relación con la adquisición de una lengua extranjera (inglés) y la aplicación en la cualificación "0612-14-03-4-01 Ciberseguridad". La persona debe dominar las siguientes competencias lingüísticas:

Nivel intermedio alto

Comprensión auditiva:

• Distingue el idioma estándar expresado, en persona o trasmitido por diferentes medios de comunicación: sobre temas conocidos o desconocidos en contextos personal, social, académico o vocacional; la comprensión solamente puede ser influenciada o confundida por ruidos fuertes, o discursos articulados inadecuadamente o por el uso de frases idiomáticas.

Comprensión de lectura:

[3] Resultados de aprendizaje según elementos del descriptor: Autonomía y responsabilidad, interacción profesional, cultural y social. Además, se deben considerar para cada Estándar de Cualificación en particular, se requieren algunos de los siguientes: salud ocupacional, sostenibilidad ambiental, servicio a la clientela, calidad, emprendedurismo, innovación, entre otros. En este apartado se incluyen los resultados de aprendizaje de una lengua extranjera. Para efectos del diseño curricular, los resultados de aprendizaje transversales deben integrarse y evaluarse en cada competencia específica.

• Distingue textos con un alto grado de independencia, adaptando el estilo, la velocidad de lectura y finalidades, utilizando fuentes de referencia apropiadamente seleccionadas. Tiene un amplio vocabulario activo de lectura, pero puede tener alguna dificultad con modismos poco frecuentes.

Expresión escrita:

• Compone textos claros y detallados sobre una amplia serie de temas relacionados con su especialidad, sintetizando y evaluando la información y argumentos de diferentes fuentes.

Expresión oral:

• Interactúa con fluidez, precisión y eficacia sobre una amplia gama de temas, fundamentado su opinión con detalles de apoyo apropiados e ideas relevantes.

IV. Contexto laboral

16

Condiciones del contexto laboral:

Condiciones del contexto laboral:

- Trabajar bajo presión y por resultados.
- Trabajar desarrollando múltiples tareas de manera simultánea.
- Trabajar sentado por largas horas utilizando equipo tecnológico.
- Trabajar con disponibilidad de horario.
- Trabajar con ética profesional.
- Trabajar con capacidad de adaptación al cambio.
- Trabajar con alta exigencia visual.
- Trabajar en los espacios georreferenciados por la organización.
- Trabajar dentro y fuera del país.
- Trasladarse a diferentes zonas del país.

17

Ámbito de aplicación de la cualificación:

- Organizaciones públicas y privadas.

18

Ocupaciones asociadas a este Estándar de Cualificación (EC) de acuerdo con Clasificador de Ocupaciones de Costa Rica (COCR):

- COCR-2011/35 Técnicos de la tecnología de la información y las comunicaciones.
- COCR-2011/351 Técnicos en operaciones de tecnología de la información y las comunicaciones y asistencia al usuario.
- COCR-2011/3511 Técnicos en operaciones de tecnología de la información y las comunicaciones.

19

Estándares de Cualificación vinculados y contenidos en el Catálogo de Cualificaciones de la EFTP-CR:

- 0612-14-01-3-01 Configuración y soporte a redes de comunicación y sistemas operativos.
- 0612-14-01-4-01 Configuración y soporte a redes de comunicación y sistemas operativos.
- 0612-14-03-3-01 Ciberseguridad.
- 0612-14-03-5-01 Análisis de Ciberseguridad.

20

Estándares de Cualificación Internacionales relacionados:

Conocer México:

- EC0995 Desarrollo de sistemas de información informáticos.
- EC1120 Mantenimiento del equipo de cómputo, diseño de redes y seguridad informática.

INCUAL:

- IFC153_3 -Seguridad Informática.
- IFC152_3 - Gestión de sistemas informáticos.
- IFC304_3 - Sistemas de gestión de información.

Ciberseguridad

- (ISC)2: CISSP - Certified Information Systems Security Professional.
- ISACA: CISM - Certified Information Security Manager.
- EC-Council: CEH - Certified Ethical Hacker.
- ISACA: CRISC - Certified in Risk and Information Systems Control.
- (ISC)2: CCSP - Certified Cloud Security Professional.
- ISACA: CISA - Certified Information Systems Auditor.

- (ISC)2: CISSP-ISSMP - Information Systems Security Management Professional.
- (ISC)2: CISSP-ISSAP - Information Systems SecurityArchitecture Professional.
- ISACA: CGEIT - Certified in the Governance of Enterprise IT.
- EC-Council: CHFI - Computer Hacking Forensic Investigator.

V. Emisión de diploma

La persona que apruebe un Programa educativo que haya sido diseñado a partir del presente Estándar de Cualificación, según el Marco Nacional de Cualificaciones de la Educación y Formación Técnica Profesional de Costa Rica, se hace acreedora al diploma de:

Ciberseguridad 0612-14-03-4-01	TÉCNICO 4
Nombre de la cualificación	Nivel de cualificación

Esta cualificación certifica que la persona es competente para:

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.

VI. Glosario de términos

Terminología asociada a la cualificación:

- **Auditoría:** Proceso mediante el cual se recopila y evalúa información acerca del funcionamiento de la arquitectura de los sistemas de información y comunicación, con el fin de obtener evidencia para determinar la integridad de los datos y la correcta funcionalidad de equipos, procesos y sistemas de almacenamiento.

- **Fases de Ciberseguridad:** Marco de trabajo que contempla políticas, procedimientos, metodologías, planes, herramientas, equipos y sistemas para manejar de manera adecuada y disminuir los riesgos en ciberseguridad. Cada fase tiene objetivos bien definidos y se pueden reconocer las siguientes: identificación, protección, detección, respuesta y recuperación.

- **Ingeniería Social:** Técnica mediante la cual un atacante convence a un tercero de revelar información sensible o confidencial sin percatarse de que existe un riesgo de seguridad y que puede ser utilizada con fines maliciosos.

MARCO NACIONAL DE CUALIFICACIONES
EDUCACIÓN Y FORMACIÓN TÉCNICA PROFESIONAL
COSTA RICA

Para más información
haga clic aquí

www.cualificaciones.cr

Volver al
INICIO

Retrocede

Volver al ÍNDICE