El estándar de cualificación **7-INCO-ITS-010 – "Diseño y desarrollo de soluciones de ciberseguridad"** es el referente para el diseño de oferta educativa que conduce al título de magíster en Diseño y desarrollo de soluciones de ciberseguridad, que responde a:

El posicionamiento de las tecnologías de la información en el sector de las TIC para el manejo de datos frente al avance de los desarrollos tecnológicos establece la necesidad de manejar modelos de soluciones de ciberseguridad en la red evitando pérdidas de datos o usos indebidos y perjudiciales de los mismos.
Los nuevos requerimientos de cualificaciones del talento humano en competencias relacionadas con la planificación, diseño, implementación de sistemas, procesos y soluciones de ciberseguridad, desarrollo de aplicaciones de software cumpliendo los requerimientos para la gestión de riesgos de seguridad e implementación de la investigación, innovación y desarrollo tecnológico aplicando los indicadores y normativa técnica del sector TIC, para así disminuir las brechas de la competitividad frente a las expectativas del sector productivo.

Al comportamiento de la prospectiva del mercado laboral, la cual muestra que los cargos derivados de esta revolución tecnológica aumentaran, como se evidencia en los resultados del estudio de identificación de brechas de capital humano entorno a las competencias para el sector TIC con enfoque en la explotación de datos realizado en 2019 por el Ministerio de Tecnologías de la Información y las Comunicaciones, teniendo en cuenta que existe una alta demanda de cargos, bajo número de aspirantes, candidatos que no cumplen con las competencias requeridas por las empresas en el contexto nacional y regional.

Las brechas de talento humano en relación con la calidad muestran la importancia de fortalecimiento de competencias en: análisis y alcance de la ciber estrategia de seguridad, vectores de amenaza, técnicas de hacking ético, pruebas de penetración, definición de los lineamientos de seguridad del código fuente de la aplicación de software y de técnicas forenses en la recopilación de evidencias de un ataque informático.

Los estándares nacionales e internacionales emanados por los respectivos organismos que rigen la parte legal y normativa, en relación con componentes tecnológicos. Y competencias del talento humano en referentes de países tales como Colombia - Sena, Argentina, Chile y México.

<table>
<tr><th colspan="3">1. IDENTIFICACIÓN DE LA CUALIFICACIÓN</th></tr>
<tr><td colspan="2">Código de la cualificación: 7-INCO-ITS-010</td><td>Versión:
01 – 2020</td><td>Fecha Aprobación: (dd) de (mes) de (aaaa)
Estado: en construcción.</td></tr>
<tr><td>DENOMINACIÓN</td><td colspan="3">Diseño y desarrollo de soluciones de ciberseguridad.</td></tr>
<tr><td>NIVEL DEL MNC</td><td colspan="3">7</td></tr>
<tr><td>ÁREA DE CUALIFICACIÓN</td><td colspan="3">Informática y Comunicaciones -INCO.</td></tr>
<tr><td>DURACIÓN (horas-créditos)</td><td colspan="3">35 a 75 créditos – 1680 a 3600 horas.</td></tr>
<tr><td>Organismo que autoriza la cualificación</td><td colspan="3"></td></tr>
<tr><td>Institución que otorga la cualificación</td><td colspan="3"></td></tr>
<tr><td>Cualificación conducente a:</td><td colspan="3">Título de magíster.
(Ley 30 de 1992 y decreto 1001 de 2006).</td></tr>
<tr><th colspan="4">2. PERFIL DE COMPETENCIAS</th></tr>
<tr><td>COMPETENCIA GENERAL</td><td colspan="3">Planificar, diseñar, desarrollar, implantar y gestionar soluciones de ciberseguridad salvaguardando los activos de información e infraestructura tecnológica de la organización mediante la investigación de incidentes de seguridad, aplicación de políticas y normativa de protección de datos e innovando en técnicas y herramientas que permitan mitigar los riesgos de seguridad asegurando la continuidad del negocio.</td></tr>
<tr><td>ÁMBITO PRODUCTIVO</td><td colspan="3">Esquema cadena de valor:
 

Subsector de Tecnologías de la Información, apoyado en el pilar de Infraestructura (despliegue, Instalación y Administración).
Sector productivo:
Sector Tecnologías de la Información y de las Telecomunicaciones
Subsector Tecnologías de la Información, Telecomunicaciones, Software.

Contexto de acción: Empresas de cualquier sector productivo, públicas o privadas, productivas o de servicios. Creando estrategias de ciberdefensa. Desempeñándose como analista, director, especialista, arquitecto de ciberseguridad en el área de las tecnologías de la información y las comunicaciones, manteniendo la continuidad operacional de los servicios que presta la red y los niveles de seguridad requeridos por el negocio.
Departamentos y empresas de sistemas e informática que requieren supervisar la ejecución de proyectos relacionados con ciberseguridad.
Centros de operaciones de Ciberseguridad.
En el área de la seguridad informática del departamento TI de grandes, medianas y pequeñas organizaciones.
Maneja su propia empresa prestando servicios o consultoría en ciberseguridad, formulando y generando proyectos de investigación e innovación en el sector de las TIC.
Ocupaciones relacionadas:</td></tr>
</table>

	2529 - Profesionales en bases de datos y en redes de computadores no clasificados en otros grupos primarios • Administrador de seguridad informática. • Analista de seguridad de computadores. • Analista de seguridad de datos. • Analista de seguridad de las TIC. • Consultor de análisis forense digital. • Consultor de seguridad de datos. • Consultor de seguridad de equipo informático. • Consultor de seguridad de las TIC. • Consultor de seguridad informática. • Especialista en análisis forense digital. • Especialista en seguridad de información. • Especialista en seguridad de las TIC. • Especialista en seguridad informática. • Especialista forense digital. • Auditor de sistemas. **Otras denominaciones:** • Director de seguridad de la información. • Analista de seguridad informática. • Oficial de seguridad informática. • Experto en seguridad informática. • Oficial de seguridad de la información. • Especialista en seguridad informática.
COMPETENCIAS ESPECÍFICAS	**CE01-7-INCO-TIC-010-**Planificar las soluciones de ciberseguridad de acuerdo con metodologías y normativa técnica.
	CE02-7-INCO-TIC-010-Diseñar el sistema de gestión de la seguridad de la información de acuerdo con metodologías de referencia y normatividad técnica del sector TIC.
	CE03-7-INCO-TIC-010-Desarrollar aplicaciones de software acorde con los requerimientos de seguridad, buenas prácticas y normativa técnica del sector TIC.
	CE04-7-INCO-TIC-010-Implantar sistemas y procesos de ciberseguridad de acuerdo con estrategias del negocio y normativa técnica del sector TIC.
	CE05-7-INCO-TIC-010-Administrar los riesgos de ciberseguridad en entornos empresariales e industriales de acuerdo con metodologías y buenas prácticas de referencia.
	CE06-7-INCO-TIC-010-Implementar la investigación, innovación y desarrollo en el sector de las tecnologías de la información y las comunicaciones de acuerdo con requerimientos y tendencias de la industria.
COMPETENCIA ESPECIFICA	**CE01-7-INCO-TIC-010-**Planificar las soluciones de ciberseguridad de acuerdo con metodologías y normativa técnica.
Elemento de competencia 1: Diagnosticar los requerimientos de seguridad de acuerdo con criterios técnicos y organizacionales. **Criterios de desempeño:** • La determinación del contexto organizacional está acorde con técnicas de análisis y tipo de negocio. • La identificación de las necesidades de ciberseguridad cumple con requerimientos de la organización y criterios técnicos. • El análisis de la regulación en seguridad de la información está acorde con el tipo de organización.	

- La evaluación de las políticas de seguridad de la información corresponde con procedimientos técnicos y protocolos de la organización.
- La definición de los objetivos de la ciber estrategia de seguridad está acorde con estándares y modelo operativo del negocio.
- La delimitación del alcance de la ciber estrategia de seguridad está acorde con los requerimientos técnicos y la continuidad del negocio.
- La definición del marco metodológico corresponde con las necesidades de la organización y referentes técnicos.
- La identificación de los activos, procesos e información está acorde con metodologías técnicas y estrategias del negocio.

Elemento de competencia 2: Identificar amenazas y vulnerabilidades de los activos de información e infraestructura TI de acuerdo con metodologías y normativa técnica del sector TIC.

Criterios de desempeño:

- La detección de amenazas contra la información y la infraestructura tecnológica cumple con metodología y procedimientos técnicos.
- La identificación de alertas tempranas y nuevas amenazas está acorde con procedimientos técnicos.
- La identificación de vectores de amenazas está acorde con metodologías y procedimientos técnicos.
- La utilización de herramientas de software para la detección de amenazas cumple con la estrategia de ciberseguridad y del negocio.
- La identificación de vulnerabilidades sobre los activos de información está acorde con procedimientos técnicos y metodología de referencia.
- La aplicación de herramientas de escaneo de vulnerabilidades está acorde con metodologías y procedimientos técnicos.
- La aplicación de técnicas de hacking ético está acorde con metodologías y procedimiento técnico.
- La realización de pruebas de penetración a los sistemas informáticos cumple con metodologías y procedimiento técnico.

Elemento de competencia 3: Determinar los riesgos de seguridad de los activos de información e infraestructura tecnológica según metodologías y normativa técnica del sector TIC.

Criterios de desempeño:

- La identificación de los riesgos de seguridad está acorde con metodologías de análisis y criterios técnicos.
- La definición de la probabilidad de ocurrencia de un riesgo de seguridad cumple con criterios técnicos y métodos de análisis de riesgos.
- La valoración del impacto de la materialización de los riesgos de seguridad cumple con criterios técnicos y marcos de referencia.
- La medición de riesgos de seguridad de la información está acorde con metodologías de análisis y criterios técnicos.
- La descripción de las consecuencias de la materialización de los riesgos de seguridad cumple con criterios técnicos y los objetivos del negocio.
- La socialización del análisis de riesgos de seguridad de la información corresponde con los protocolos de la organización y criterios técnicos.

Elemento de competencia 4: Planear la seguridad de los sistemas informáticos de acuerdo con los requerimientos técnicos y organizacionales.

Criterios de desempeño:

- La planificación de la estrategia de ciberseguridad cumple con estándares, políticas y modelo operativo del negocio.

- La integración de la ciber estrategia de seguridad con la estrategia del negocio está acorde con estándares y lineamientos organizacionales.
- La definición de actividades y responsables de la ciberseguridad está acorde con lineamientos organizacionales y la continuidad del negocio.
- La aplicación de un modelo de defensa en profundidad está acorde con buenas prácticas en seguridad y estrategia del negocio.
- La definición de parámetros de seguridad en equipos y dispositivos informáticos de la red está acorde con criterio técnico y resultados del análisis de riesgos.
- La elección de protocolos de seguridad en la red cumple con normativa y procedimiento técnico.
- La definición de los controles de acceso a los sistemas de información e infraestructura TI está acorde al establecimiento de mínimos privilegios y requerimientos organizacionales.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, software de monitoreo de red y de detección de amenazas, herramientas de diagnóstico en seguridad de la información y herramientas de escaneo de vulnerabilidades.

- **Productos y resultados (evidencias):**
  Los objetivos y el alcance de la ciber estrategia de seguridad.
  Identificación de los activos, procesos e información a incluir en la ciber estrategia de seguridad.
  Aplicación de técnicas de hacking ético.
  Realización de pruebas de penetración.
  Valoración del impacto de la materialización de los riesgos de seguridad.
  Análisis de riesgos de seguridad de la información.
  La planeación de la estrategia de ciberseguridad.

- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Políticas de seguridad de la información en la organización.
  Requerimientos técnicos.

COMPETENCIA ESPECIFICA	**CE02-7-INCO-TIC-010-**Diseñar el sistema de gestión de la seguridad de la información de acuerdo con metodologías de referencia y normatividad técnica del sector TIC.

Elemento de competencia 1: Proyectar el plan de gestión de riesgos de seguridad de la información de acuerdo con metodologías de referencia y normatividad técnica del sector TIC.

Criterios de desempeño:

- El seguimiento de la legislación y normatividad de la seguridad de la información cumple con procedimientos técnicos y organizacionales.
- La definición de la política de seguridad de la información está acorde con la normativa del sector TIC y las necesidades de la organización.
- La descripción del plan de tratamiento de riesgos cumple con referentes técnicos y normativa jurídica que regula la seguridad informática.
- La asignación de recursos para el tratamiento de riesgos de seguridad de la información está acorde con procedimientos técnicos.
- La definición de indicadores de valoración de la efectividad del plan de tratamiento de riesgos y controles asociados a la seguridad de la información está acorde con procedimientos y normativa técnica del sector TIC.
- El establecimiento del cronograma de actividades para la implementación del sistema de gestión de seguridad de la información está acorde con los recursos del proyecto.
- La documentación del plan de gestión de riesgos de seguridad de la información está acorde con metodologías y criterios técnicos.

• La aprobación del plan de gestión de riesgos de seguridad de la información está acorde con el compromiso de la alta gerencia y estrategia de continuidad del negocio.
Elemento de competencia 2: Construir el plan de gestión de incidentes de seguridad de la información de acuerdo con estándares técnicos de referencia y la estrategia de continuidad del negocio. **Criterios de desempeño:** • La formulación del plan de gestión de incidentes está acorde con criterio y metodología técnica de referencia. • La definición de procedimientos de detección, análisis, contención, erradicación y recuperación en el plan de gestión de incidentes de seguridad cumple con procedimiento técnico y metodología de referencia. • La clasificación de incidentes de seguridad y su grado de criticidad está acorde con criterio técnico y metodología de referencia. • La revisión del plan de gestión de incidentes está acorde con procedimientos técnicos y metodología de referencia. • El establecimiento de indicadores de efectividad del plan de gestión de incidentes de seguridad de la información está acorde con procedimientos técnicos. • La asignación de recursos para la gestión de incidentes corresponde con el procedimiento de contención y mitigación de incidentes. • La documentación del plan de gestión de incidentes de seguridad de la información cumple con metodología técnicas de referencia y estrategia de continuidad del negocio.
Elemento de competencia 3: Establecer el plan de capacitación y educación en seguridad de la información de acuerdo con políticas y estándares técnicos de referencia. **Criterios de desempeño:** • La definición de la estrategia de gestión de cambio y formación en seguridad de la información está acorde con lineamientos organizacionales y criterio técnico. • La elaboración del programa de gestión de cambio y sensibilización en seguridad de la información cumple con la política de seguridad y normativa técnica del sector TIC. • La formulación de las actividades de capacitación en seguridad de la información está acorde con el plan de tratamiento de riesgos y metodologías de referencia. • La verificación de la efectividad de la sensibilización y educación en seguridad de la información cumple con la política de seguridad e indicadores del plan de capacitación. • La documentación del programa de gestión de cambio, sensibilización y capacitación está acorde con la política de seguridad de la información y lineamientos organizacionales.
Contexto de la competencia • **Recursos utilizados:** Computadores, software de aplicación, herramientas de software para la detección de amenazas, software para gestionar cronogramas y de escaneo de vulnerabilidades. • **Productos y resultados (evidencias):** Plan de gestión de riesgos de seguridad de la información. Definir y asignar los recursos para el tratamiento de riesgos de seguridad. Generar el cronograma de implementación del sistema de gestión de seguridad de la información. Realizar el plan de gestión de incidentes incluyendo indicadores de efectividad. • **Información requerida (Referentes):** Normatividad técnica y jurídica en seguridad de la información. Información de la estrategia de continuidad del negocio.

COMPETENCIA ESPECIFICA	**CE03-7-INCO-TIC-010-**Desarrollar aplicaciones de software acorde con los requerimientos de seguridad, buenas prácticas y normativa técnica del sector TIC.

Elemento de competencia 1: Definir los lineamientos de seguridad del código fuente de la aplicación de software de acuerdo con buenas prácticas y metodología.

Criterios de desempeño:

- La elección de la metodología de desarrollo seguro está acorde a procedimientos técnicos.
- La selección del modelo de desarrollo seguro de aplicaciones de software cumple con normativa técnica del sector TIC.
- La determinación de los requerimientos funcionales de la aplicación de software está acorde con las necesidades de la organización y metodología.
- La verificación de los requerimientos no funcionales de la aplicación de software corresponde con metodología y normativa técnica del sector TIC.
- El establecimiento de los controles de seguridad en el ciclo de vida del desarrollo cumple normativa del sector TIC y estándares técnicos.
- La elaboración del plan de pruebas al código de la aplicación de software cumple con metodología y estándares técnicos.

Elemento de competencia 2: Crear la aplicación de software seguro de acuerdo con metodologías y normativa técnica del sector TIC.

Criterios de desempeño:

- El aseguramiento del ambiente de desarrollo cumple con normativa técnica del sector TIC y metodología.
- La identificación de criterios de seguridad en el código cumple con estándares técnicos y requerimientos organizacionales.
- La incorporación de mecanismos de seguridad en el desarrollo de la aplicación cumple con metodología y procedimiento técnico.
- La integración de técnicas de codificación y escapado de datos corresponde con metodología y procedimiento técnico.
- El aseguramiento de la calidad del código fuente está acorde con criterios técnicos y de seguridad de la información.
- La implementación de medidas de protección para realizar consultas a bases de datos está acorde con la tecnología y plataforma utilizada.
- La implementación de mecanismos de autenticación seguros cumple con metodología y requerimientos de la organización.
- La validación de los criterios de seguridad en las bases de datos cumple con el modelo de desarrollo seguro y de seguridad de la información.

Elemento de competencia 3: Probar la seguridad del código de la aplicación de software de acuerdo con estándares y procedimientos técnicos.

Criterios de desempeño:

- La validación de los datos en el desarrollo de la aplicación cumple con los requerimientos de sintáctica y semántica.
- El uso de herramientas de escaneo de vulnerabilidades de aplicación cumple con procedimiento técnico y normativa del sector TIC.
- La ejecución de pruebas de penetración (Hacking Ético) a la aplicación de software está acorde con metodología y procedimiento técnico.
- La identificación de las vulnerabilidades y riesgos de seguridad del desarrollo está acorde con el análisis de los requerimientos funcionales, no funcionales y metodología.
- La corrección de las debilidades en el código fuente está acorde con los resultados del escaneo de vulnerabilidades y test de penetración.

- La verificación de los controles de seguridad cumple con el aseguramiento y certificación de calidad del software.
- La aplicación de auditorías de software durante el desarrollo de la aplicación cumple con procedimientos técnicos y metodología.

Elemento de competencia 4: Documentar el desarrollo de la aplicación de software seguro de acuerdo con normas, estándares y marcos de referencia.

Criterios de desempeño:

- La documentación de la seguridad en el ciclo de desarrollo seguro está acorde con el modelo seleccionado y normativa técnica del sector TIC.
- El registro de vulnerabilidades y riesgos de seguridad identificados en los requerimientos funcionales y no funcionales cumple con procedimientos técnicos y metodología.
- El reporte de la ejecución y resultados del plan de pruebas al código cumple con metodología y procedimientos técnicos.
- El registro del aseguramiento de la calidad del código está acorde con la estrategia de aseguramiento de la calidad y metodología.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, software de programación y herramientas de escaneo de vulnerabilidades.

- **Productos y resultados (evidencias):**
  Generación de controles de seguridad en el ciclo de vida del software.
  Implementación de mecanismos de autenticación seguros.
  Establecimiento de los criterios de seguridad en las bases de datos.
  La aplicación de pruebas de penetración.
  Desarrollo de auditorías de software y estrategias de aseguramiento de la calidad del código.
  El registro de vulnerabilidades y riesgos de seguridad.

- **Información requerida (Referentes):**
  Documento que contenga la estrategia de continuidad del negocio.
  Normatividad técnica y jurídica en seguridad de la información.
  Política de seguridad de la información y lineamientos organizacionales.
  Normatividad técnica de desarrollo de software.

COMPETENCIA ESPECIFICA	**CE04-7-INCO-TIC-010-**Implantar sistemas y procesos de ciberseguridad de acuerdo con estrategias del negocio y normativa técnica del sector TIC.

Elemento de competencia 1: Desplegar los mecanismos de seguridad de acuerdo con normativa del sector TIC y procedimientos técnicos.

Criterios de desempeño:

- La interpretación de aspectos legales y normativa de referencia en la evaluación de la seguridad está acorde con metodología y la estrategia de ciberseguridad.
- La implementación de los sistemas y procesos de ciberseguridad cumple con normatividad técnica del sector TIC y requerimientos organizacionales.
- La aplicación de protocolos criptográficos y uso de herramientas de seguridad está acorde con procedimientos técnicos y estrategia de ciberseguridad.
- El uso de protocolos de autenticación está acorde con procedimientos técnicos y lineamientos organizacionales.
- La protección de equipos y dispositivos informáticos en la red está acorde con normativa del sector TIC y procedimientos técnicos.

- La integración de dispositivos de seguridad de red cumple con criterio técnico y buenas prácticas de referencia.
- La aplicación del backup de información está acorde con la metodología y criticidad de la información.
- La disposición de controles de navegación de usuarios a internet está acorde con metodología, políticas y lineamientos organizacionales.

Elemento de competencia 2: Examinar la efectividad de los mecanismos de seguridad de acuerdo con indicadores y normativa técnica del sector TIC.

Criterios de desempeño:

- La valoración de los controles de seguridad a terceros cumple con criterio técnico y normativa del sector TIC.
- La medición de la efectividad de los controles de seguridad cumple con procedimientos técnicos.
- La aplicación de técnicas de análisis forense está acorde con normativa del sector TIC y procedimiento técnico.
- El uso de técnicas de hacking ético está acorde con procedimientos técnicos y normativa jurídica que regula la seguridad informática.
- La realización de pruebas de pentesting de caja blanca, gris y negra cumple con requerimientos de la organización y normativa jurídica que regula la seguridad informática.
- La utilización de honeypots está acorde con criterio y procedimiento técnico.
- El proceso de auditoria de los sistemas de información e infraestructura TI está acorde con estándares y buenas prácticas de referencia.

Elemento de competencia 3: Aplicar acciones de mejora en la ciberseguridad de acuerdo con metodología y auditoria de seguridad.

Criterios de desempeño:

- La corrección de hallazgos de seguridad en los sistemas informáticos está acorde con los resultados de las pruebas técnicas de hacking ético y metodología.
- La parametrización de los controles físicos o lógicos en el ciber entorno cumple con procedimientos técnicos y requerimientos organizacionales.
- La implementación de nuevos controles de ciberseguridad corresponde con criterios técnicos y normativa del sector TIC.
- La ejecución de acciones preventivas y correctivas en la estrategia de ciberseguridad cumple con procedimientos técnicos y requerimientos de la organización.
- La reconfiguración para el aseguramiento del ciber entorno está acorde con la valoración de los mecanismos de seguridad y procedimiento técnico.

Elemento de competencia 4: Socializar los resultados de la estrategia de ciberseguridad de acuerdo con la metodología y requerimientos organizacionales.

Criterios de desempeño:

- La presentación de resultados de la estrategia de ciberseguridad cumple con los requerimientos técnicos de la organización.
- La documentación de la solución está acorde con normativa del sector TIC y requerimientos de la organización.
- La finalización de la implantación de los sistemas y procesos de ciberseguridad cumple con procedimientos técnicos y marcos de referencia.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, software de monitoreo y de auditoria.

- **Productos y resultados (evidencias):**
  Aplicar el plan de tratamiento y gestión de los riesgos.
  Implementación de la estrategia de ciberseguridad.

La definición y aplicación de backup de información.
Evaluación de los controles de seguridad.
Aplicación de técnicas de análisis forenses y hacking ético.
Documentación y presentación de los resultados de la implementación de la estrategia de ciberseguridad.

- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Política de seguridad de la información y lineamientos organizacionales.
  Estrategia de ciberseguridad.

COMPETENCIA ESPECIFICA	**CE05-7-INCO-TIC-010-**Administrar los riesgos de ciberseguridad en entornos empresariales e industriales de acuerdo con metodologías y buenas prácticas de referencia.

Elemento de competencia 1: Monitorear el sistema de gestión de seguridad de la información de acuerdo con procedimientos técnicos y metodología de referencia.

Criterios de desempeño:

- La vigilancia de los vectores de ataque abiertos corresponde con criterios y procedimientos técnicos.
- La aplicación de pruebas de penetración cumple con metodologías y procedimientos técnicos.
- El seguimiento de los eventos de seguridad e intrusión cumple con metodología y procedimientos técnicos.
- La revisión de los logs y registro de eventos está acorde con procedimientos técnicos y metodología.
- El análisis de los vectores de ataque empleados por malware está acorde con especificaciones y criterios técnicos.
- El análisis de registro de eventos y detección de intentos de intrusión está acorde con criterios técnicos y buenas prácticas.
- La valoración de la gestión de información de eventos de seguridad (SIEM) cumple con metodología y criterio técnico.

Elemento de competencia 2: Prevenir ataques informáticos que comprometan los activos de información y ciber entornos acorde a metodologías y buenas prácticas de referencia.

Criterios de desempeño:

- La detección de ataques y violaciones de seguridad cumple con procedimientos técnicos y normativa del sector TIC.
- La organización de pruebas de Hacking Ético está acorde con las estrategias de ciberseguridad y requerimientos organizacionales.
- La utilización de herramientas de detección y prevención de intrusos está acorde con criterios y procedimientos técnicos.
- La aplicación de auditorías de seguridad está acorde con procedimientos técnicos y estrategia de continuidad del negocio.
- La actualización de la política de seguridad asociada a las contraseñas cumple con criterios técnicos y lineamientos organizacionales.

Elemento de competencia 3: Reaccionar a ataques informáticos acorde con metodologías y buenas prácticas de referencia.

Criterios de desempeño:

- El análisis de incidentes de ciberseguridad está acorde con la metodología y buenas prácticas de referencia.
- El establecimiento de las medidas de contención y seguridad para mitigar los ataques a la red cumple con metodologías y procedimientos técnicos.
- La detección y reporte de los riesgos de seguridad materializados sobre la infraestructura tecnológica está acorde con metodologías de referencia y procedimientos técnicos.

- Los procedimientos de recuperación ante un ataque de seguridad cumplen con políticas técnicas y organizacionales.
- La respuesta a los ataques de seguridad de la información de la organización está acorde con el plan gestión de incidentes y políticas de seguridad de la organización.

Elemento de competencia 4: Indagar los incidentes de ciber seguridad de acuerdo con buenas prácticas de referencia y normativa del sector TIC.

Criterios de desempeño:

- El análisis forense de las consecuencias que ha producido el ataque a los sistemas informáticos está acorde con procedimientos técnicos y normativa del sector TIC.
- La aplicación de técnicas forenses en la recopilación de evidencias de un ataque informático está acorde con procedimientos técnicos.
- La reconstrucción de la secuencia temporal del ataque cibernético cumple con procedimientos técnicos y normativa del sector TIC.
- La identificación de las causas del ataque informático está acorde con criterios y procedimientos técnicos.
- La evaluación del impacto en el sistema informático está acorde con procedimientos técnicos y metodología de referencia.
- La documentación del incidente de seguridad y los resultados obtenidos en la investigación corresponde con políticas de la organización.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, software de monitoreo y herramientas de detección y prevención de intrusos.

- **Productos y resultados (evidencias):**
  Registro y seguimiento a los eventos de seguridad e intrusión.
  Implementación de auditorías de seguridad.
  Conocimiento de procedimientos y respuesta ante los ataques de seguridad.
  Aplicación de técnicas forenses en la recopilación de evidencias de un ataque informático.
  Documentación de los incidentes de seguridad.

- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Plan gestión de incidentes y lineamientos organizacionales.

COMPETENCIA ESPECIFICA	**CE06-7-INCO-TIC-010**-Implementar la investigación, innovación y desarrollo en el sector de las tecnologías de la información y las comunicaciones de acuerdo con requerimientos y tendencias de la industria.

Elemento de competencia 1: Formular la investigación en tecnologías de la información y las comunicaciones acorde con modelos de diagnóstico y objetivo base.

Criterios de desempeño:

- La identificación de la naturaleza de la investigación corresponde con requerimientos del proyecto TIC y metodologías.
- La definición de los objetivos de la investigación en TIC está acorde con el método científico.
- La organización de las fases de investigación corresponde con metodologías y requerimientos del proyecto TIC.
- La selección de actividades de investigación cumple con los objetivos del proyecto TIC y requerimientos metodológicos.
- La adaptación del modelo de investigación del proyecto TIC está acorde con procedimientos metodológicos y técnicos.

- La proyección de los recursos de la investigación TIC corresponde con la naturaleza del proyecto.
- La instrumentación de la investigación cumple con metodologías y objetivos del proyecto TIC.

Elemento de competencia 2: Estructurar la investigación en el sector de las tecnologías de la información teniendo en cuenta metodologías de investigación y lineamientos de la gestión del proyecto.

Criterios de desempeño:

- La apropiación de la vigilancia tecnológica en el sector TIC está acorde con el plan de innovación y herramientas de búsqueda.
- La elaboración del perfil del proyecto de investigación en el sector TIC está acorde con criterios técnicos y normativas.
- La ejecución de las fases de investigación en el sector TIC está conforme con la planeación y metodologías.
- La aplicación de técnicas de investigación en el sector TIC corresponde con modelo técnico de investigación.
- La documentación de la información del proyecto TIC cumple con procedimientos técnicos y metodológicos.
- La verificación de los productos del proyecto de investigación TIC cumple con normas y procedimientos técnicos.

Elemento de competencia 3: Evaluar la investigación en el sector de las tecnologías de la información de acuerdo con metodología y lineamientos de gestión del proyecto.

Criterios de desempeño:

- El seguimiento a la investigación está acorde con la planeación y objetivos del proyecto de investigación TIC.
- El establecimiento de los lineamientos de evaluación del proyecto de investigación TIC corresponde con el plan de trabajo evaluativo.
- El diseño de instrumentos de medición del proyecto de investigación TIC cumple con criterios de evaluación y metodología.
- La aplicación de instrumentos de medición al proyecto de investigación TIC cumple con los objetivos del proyecto.
- El análisis de los resultados del proyecto de investigación TIC cumple con procedimientos técnicos y normativa.
- La descripción de resultados del proyecto de investigación TIC corresponde con el alcance y objetivos del proyecto.
- La ejecución del plan de mejoramiento del proyecto de investigación TIC cumple con los lineamientos y norma técnica.

Elemento de competencia 4: Gestionar los resultados del proyecto en el sector de las tecnologías de la información de acuerdo con criterios técnicos y la metodología de investigación.

Criterios de desempeño:

- El alistamiento de la documentación del proyecto de investigación TIC está acorde con metodología y contexto normativo.
- La presentación de la documentación de la solución del proyecto de investigación TIC cumple con metodología y contexto normativo.
- La difusión de resultados del proyecto de investigación TIC está acorde con los criterios técnicos y normativa.
- La transferencia de conocimiento de los resultados del proyecto de investigación TIC cumple con metodología y contexto normativo.
- La formalización de los productos del proyecto de investigación TIC cumple con metodología y contexto normativo.

Contexto de la competencia

- **Recursos utilizados:** Computadores con conexión a Internet, software de aplicación y herramientas de seguimiento y administración de tareas.

- **Productos y resultados (evidencias):**
  Plan de trabajo de investigación.
  Organización de las fases de investigación y elaboración del cronograma del proyecto.
  Aplicación de técnicas de investigación.
  Análisis y descripción de los resultados del proyecto de investigación TIC.
  Documentación de la solución del proyecto de investigación TIC.

- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Modelos de investigación.
  Técnicas de investigación.
  Recursos disponibles en la organización.
  Estándares y políticas de calidad.

COMPETENCIAS CLAVE (Básicas y transversales)

Competencias Básicas

Competencia	Duración
Comunicación y Solución de problemas: • Escucha activa. • Comunicación asertiva. • Empatía. • Comunicación gestual. • Semiología. • Respuestas oportunas a los requerimientos del mercado. • Habilidades comunicativas. • Habilidades lecto escritoras en comunicación tecnológica. • Dominio técnico del idioma inglés. • Habilidades de comunicación en segunda lengua, inglés. • Estrategias para la solución y prevención de problemas. • Evaluación de causas y efectos de problemas. • Toma de decisiones. • Sesiones grupales, para lluvias de ideas. • Técnicas creativas para la solución de problemas. • Enfoque sistémico en la solución de problemas. • Situaciones y alternativas de solución. • Acciones concretas para solucionar problemas. • Viabilidad para el aprovechamiento de oportunidades.	48 horas/ 1 crédito
Liderazgo y Trabajo en equipo: • Capacidad analítica y crítica constructiva. • Consecución de metas y objetivos. • Creación de ambientes de confianza laboral. • Integración de nuevos miembros al ambiente laboral. • Sentido de compromiso y responsabilidades. • Manejo de diversidad de opiniones. • Planeación del tiempo. • Equidad de género. • Asignación de trabajos y cargas equitativas. • Manejo de información compartida. • Crea compromiso y movilización de los miembros del equipo.	48 horas/ 1 crédito

	• Gestión y aceptación de retos y desafíos. • Directrices para alcanzar metas. • Motivación a los equipos de trabajo. • Buenas prácticas y desempeños en la calidad de vida laboral. • Generación y manejo del clima laboral positivo en un entorno de inclusión. • Comunicación asertiva en entornos de respeto. • Situaciones y escenarios futuros de la organización.	
	Creatividad y Proactividad: • Situaciones y alternativas de solución para la toma de decisiones. • Contribución de nuevos elementos. • Investigación y documentación sobre dinámica de las organizaciones y su competitividad en el mercado.	48 horas/ 1 crédito
	Calidad y Planeación: • Capacidad de síntesis, objetividad y agilidad para tomar decisiones. • Orden y meticulosidad en la inspección y elaboración de registros. • Capacidad de establecer la trazabilidad de un producto. • Planeación de la documentación necesaria para asegurar y controlar la calidad de los productos y servicios. • Adaptación a los procesos de mejora continua y buenas prácticas. • Actividades de gestión de calidad.	48 horas/ 1 crédito
	Informática: • Herramientas de manejo de proyectos. • Curación de información a través de plataformas móviles. • Análisis de información en la toma de decisiones.	48 horas/ 1 crédito
	Lógica de programación y Matemáticas: • Herramientas de desarrollo. • Paradigmas de programación. • Aptitud matemática. • Planteamiento de problemas matemáticos. • Relación de las matemáticas a la solución de problemas de la industria. • Descripción de modelos matemáticos, aplicados a la solución de problemas. • Aplicación de software de modelización de fenómenos y soluciones particulares. • Visualización de datos de expresiones matemáticas en la solución de problemas.	96 horas/ 2 créditos
	Ciencias naturales y Ética: • Experimentos aplicados a las TIC. • Fenómenos naturales aplicados a las TIC. • Método científico y diseño experimental. • Hallazgos experimentales de ciencias naturales aplicadas.	48 horas/

	• Entorno natural. • Hipótesis y variables de trabajo. • Diseño y propuesta de soluciones. • Profesionalismo. • Autodisciplina. • Puntualidad. • Cumplimiento de normas en el ámbito laboral. • Capacidad de análisis, síntesis y criticidad. • Código de ética. • Imparcialidad, objetividad e igualdad en el ambiente laboral. • Respeto.	1 crédito

Competencias Transversales

Nombre de la Competencia Transversal		
Módulo	**Resultados de Aprendizaje**	**Duración**
Incorporar las políticas de protección ambiental	**RA1.** Determina el alcance del sistema de gestión ambiental en la organización de acuerdo con la política medio ambiental. **RA2.** Vela por el cumplimiento de la política de protección ambiental según las necesidades de la organización y la normatividad vigente. **RA3.** Valora los resultados de la implementación de las políticas de protección ambiental según los impactos en la organización y el entorno. **RA4.** Diseña estrategias de tratamiento de riesgos para aminorarlos o suprimirlos acorde con los proyectos de la organización y la normativa vigente.	144 horas/ 3 créditos
Cultura emprendedora y empresarial Proponer ideas y buscar oportunidades	**RA1.** Monitorea tendencias relevantes analizando las oportunidades y amenazas para generar valor y transforma las ideas en soluciones que aportan valor.	
Cultura emprendedora y empresarial Manejar recursos	**RA2:** Diseña estrategias de desarrollo profesional para el equipo y la organización basado en una comprensión clara de las fortalezas y debilidades, en relación con las oportunidades actuales y las futuras para crear valor.	144 horas/ 3 créditos

	Cultura emprendedora y empresarial Educación financiera y económica	**RA3:** Evalúa la salud financiera de una actividad de creación de valor y emite concepto sobre flujo de fondos de una organización utilizando indicadores financieros.	
	Cultura emprendedora y empresarial Pasar a la acción	**RA4:** Involucra e inspira a otras personas, consiguiendo que se integren en el equipo del proyecto a desarrollar y diseña un plan de acción detallado teniendo en cuenta circunstancias cambiantes y al logro de los objetivos.	
	Cultura emprendedora y empresarial Manejar la incertidumbre, la ambigüedad y el riesgo	**RA5:** Evalúa el riesgo al que la empresa está expuesta a medida que cambian las condiciones.	
	Investigación aplicada	**RA1.** Demuestra conocimiento amplio de la teoría y práctica de un campo profesional especializado en contextos multidisciplinarios. **RA2.** Aborda desde una visión sistémica los problemas o dificultades, planteando soluciones y alternativas. **RA3.** Formula soluciones innovadoras a partir de la resolución de problemas complejos mediante la investigación y valoración de información avanzada. **RA4.** Genera ambientes de innovación y herramientas que promueven el desarrollo de nuevas ideas. **RA5.** Evalúa la viabilidad, factibilidad y sostenibilidad de soluciones innovadoras, priorizando según las capacidades y recursos asignados.	96 horas/ 2 créditos

3. REFERENTES PARA LA EDUCACIÓN Y FORMACIÓN	
CE01-7-INCO-TIC-010-Planificar las soluciones de ciberseguridad de acuerdo con metodologías y normativa técnica.	
Duración créditos: 5 a 11	**Duración en horas: 240 a 528**
Resultado de aprendizaje 1. Fijar los requerimientos de ciberseguridad en las organizaciones teniendo en cuenta criterio técnico.	
Resultado de aprendizaje 2. Plantear estrategias de ciberseguridad de la información según las políticas de la organización.	
Resultado de aprendizaje 3. Reconocer las amenazas y vulnerabilidad de la red de acuerdo con criterio técnico.	

Resultado de aprendizaje 4. Manejar técnicas aplicadas a la vulnerabilidad de la red según criterio técnico.	
Resultado de aprendizaje 5. Dimensionar el riesgo de seguridad de la red teniendo en cuenta metodología de análisis de riesgos.	
Resultado de aprendizaje 6. Caracterizar el riesgo de seguridad de la red de acuerdo con criterio técnico.	
Resultado de aprendizaje 7. Organizar las actividades de ciber seguridad de la red según modelo operativo del negocio.	
Resultado de aprendizaje 8. Seleccionar modelos de ciber seguridad de la red teniendo en cuenta criterio técnico.	
CE02-7-INCO-TIC-010-Diseñar el sistema de gestión de la seguridad de la información de acuerdo con metodologías de referencia y normatividad técnica del sector TIC.	
Duración créditos: 6 a 13	**Duración en horas: 288 a 624**
Resultado de aprendizaje 1. Programar las actividades técnicas y legales para el tratamiento de riesgos teniendo en cuenta la normatividad vigente.	
Resultado de aprendizaje 2. Enfocar el plan de gestión de riesgos de seguridad de la información de acuerdo con política de la organización.	
Resultado de aprendizaje 3. Categorizar los incidentes de seguridad de la información en la red según criterio técnico.	
Resultado de aprendizaje 4. Elaborar el plan gestión de incidentes de seguridad de la información de acuerdo con criterio técnico.	
Resultado de aprendizaje 5. Hacer el plan de gestión de cambio, sensibilización y capacitación en seguridad de la información teniendo en cuenta lineamientos de la organización.	
Resultado de aprendizaje 6. Preparar estrategias para el fomento de la gestión de cambio, sensibilización y capacitación según política de seguridad de la información.	
CE03-7-INCO-TIC-010-Desarrollar aplicaciones de software acorde con los requerimientos de seguridad, buenas prácticas y normativa técnica del sector TIC.	
Duración créditos: 6 a 14	**Duración en horas: 288 a 672**
Resultado de aprendizaje 1. Analizar los componentes funcionales de la aplicación de software de acuerdo con procedimiento técnico.	
Resultado de aprendizaje 2. Proponer el plan de pruebas al código de la aplicación de software teniendo en cuenta estándares técnicos.	
Resultado de aprendizaje 3. Interpretar el entorno tecnológico para la aplicación de software según criterio técnico.	
Resultado de aprendizaje 4. Generar aplicaciones de software seguro teniendo en cuenta normativa del sector TIC.	
Resultado de aprendizaje 5. Ejecutar pruebas de seguridad a la aplicación de software según plan de pruebas.	
Resultado de aprendizaje 6. Auditar el desarrollo de la aplicación de software de acuerdo con criterio técnico.	
Resultado de aprendizaje 7. Revisar el historial documental y registro de hallazgos de seguridad de la aplicación de software según criterio técnico.	
Resultado de aprendizaje 8. Sistematizar la información del aseguramiento de la calidad de las aplicaciones de software teniendo en cuenta metodología.	
CE04-7-INCO-TIC-010-Implantar sistemas y procesos de ciberseguridad de acuerdo con estrategias del negocio y normativa técnica del sector TIC.	
Duración créditos: 6 a 13	**Duración en horas: 288 a 624**
Resultado de aprendizaje 1. Apropiar protocolos, marco legal y regulatorio de ciberseguridad de acuerdo con política organizacional.	
Resultado de aprendizaje 2. Configurar el ecosistema de ciberseguridad de la red teniendo en cuenta criterio técnico.	
Resultado de aprendizaje 3. Inspeccionar los controles del sistema de ciberseguridad de la red según criterio técnico.	

Resultado de aprendizaje 4. Reportar novedades de la inspección del sistema de ciberseguridad de la red teniendo en cuenta procedimiento técnico.
Resultado de aprendizaje 5. Solucionar problemas tecnológicos de ciberseguridad en los sistemas informáticos de acuerdo con criterio técnico.
Resultado de aprendizaje 6. Actualizar el sistema de ciberseguridad de la red TI teniendo en cuenta la normativa del sector TIC.
Resultado de aprendizaje 7. Consolidar los resultados de la aplicación de estrategias de ciberseguridad según requerimientos organizacionales.
Resultado de aprendizaje 8. Demostrar la implantación de los sistemas y procesos de ciberseguridad teniendo en cuenta criterio técnico.
CE05-7-INCO-TIC-010-Administrar los riesgos de ciberseguridad en entornos empresariales e industriales de acuerdo con metodologías y buenas prácticas de referencia.
Duración créditos: 6 a 12 | **Duración en horas: 288 a 576**
Resultado de aprendizaje 1. Visualizar el sistema de monitoreo informático de información e infraestructura de red de acuerdo con procedimiento técnico.
Resultado de aprendizaje 2. Valorar los resultados del monitoreo de los sistemas informáticos e infraestructura de red según criterio técnico.
Resultado de aprendizaje 3. Controlar puntos críticos de la ciberseguridad de la red teniendo en cuenta normatividad del sector TIC.
Resultado de aprendizaje 4. Coordinar estrategias para el manejo de contingencias en la ciberseguridad según procedimiento técnico.
Resultado de aprendizaje 5. Relacionar los riesgos de la ciberseguridad en la infraestructura tecnológica de acuerdo con procedimiento técnico.
Resultado de aprendizaje 6. Responder a los ataques a la ciberseguridad de la infraestructura tecnológica según criterio técnico.
Resultado de aprendizaje 7. Verificar la trazabilidad del incidente de ciberseguridad en la infraestructura tecnológica teniendo en cuenta procedimiento técnico.
Resultado de aprendizaje 8. Presentar los resultados de la evaluación del incidente de ciberseguridad en la infraestructura tecnológica según normativa del sector TIC.
CE06-7-INCO-TIC-010-Implementar la investigación, innovación y desarrollo en el sector de las tecnologías de la información y las comunicaciones de acuerdo con requerimientos y tendencias de la industria.
Duración créditos: 6 a 12 | **Duración en horas: 288 a 576**
Resultado de aprendizaje 1. Elaborar el estado del arte de investigación en el sector TIC según requerimientos del proyecto.
Resultado de aprendizaje 2. Hacer el protocolo de investigación en el sector TIC de acuerdo con procedimientos metodológicos.
Resultado de aprendizaje 3. Realizar el perfil del proyecto de investigación en el sector TIC de acuerdo con metodología.
Resultado de aprendizaje 4. Documentar los resultados del proyecto de investigación en el sector TIC teniendo en cuenta metodología.
Resultado de aprendizaje 5. Implantar el sistema de evaluación y mejora del proyecto de investigación en el sector TIC de acuerdo con metodología.
Resultado de aprendizaje 6. Informar los resultados de la evaluación del proyecto de investigación en el sector TIC según metodología.
Resultado de aprendizaje 7. Disponer la documentación final del proyecto de investigación en el sector TIC teniendo en cuenta la metodología.
Resultado de aprendizaje 8. Dirigir el plan de divulgación del proyecto de investigación en el sector TIC de acuerdo con metodología.

4. PARÁMETROS DE CALIDAD	
REQUISITOS DE INGRESO O ACCESO A LA CUALIFICACIÓN	Profesional universitario con título correspondiente a las áreas relacionadas con el campo de estudio.
PROFESIÓN REGULADA Y NORMATIVA ASOCIADA	Profesión regulada por Consejo Profesional Nacional de Ingeniería y afines (COPNIA), bajo la normativa: Ley 842 de 2003: mediante esta ley se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. Ley 1672 de 2013 y considera la situación y dinámicas actuales de los RAEE en Colombia.