El estándar de cualificación **6-INCO-ITS-008 – "Gestión de la seguridad de la información"** es el referente para el diseño de oferta educativa que conduce al título de especialista universitario en Gestión de la seguridad de la información, que responde a:

Los nuevos modelos de gestión de seguridad de los datos frente a las amenazas que se generan en las redes de información establecen retos para disminuir las brechas del talento humano en competencias relacionadas con: la evaluación de la seguridad de la información, planificación, diseño, implementación, mantenimiento y administración del sistema de gestión de seguridad de la información aplicando la normativa técnica y jurídica en seguridad de la información con el objetivo de preservar la integridad de la información de las diferentes organizaciones.

La oferta laboral solicitada por los portales tales como: El empleo, CompuTrabajo, LinkedIn, Tic Job y otras plataformas (Jobs, Trabajando.com, Indeed, y Aldaba), permiten evidenciar, la alta necesidad a nivel nacional y regional de personas con conocimientos en políticas de seguridad de la información, matriz de riesgos y habilidades para la implementación de sistemas de gestión de seguridad de la información.

El análisis prospectivo de la demanda de estos cargos, los cuales muestran un aumento como resultado del crecimiento de las organizaciones, la globalización de los mercados y las políticas del gobierno nacional enfrentándonos a nuevos retos con el uso de las tecnologías emergentes, los requerimientos y las necesidades del sector productivo.

Las brechas de la pertinencia del talento humano en competencias para el reconocimiento de amenazas y vulnerabilidades sobre los activos de información, análisis y plan de administración de riesgos, gestión de incidentes y auditoria al sistema de seguridad de la información.

Como referente internacional para esta cualificación se consultó la cámara de la industria Argentina del software CESSI institución dedicada al desarrollo de comisiones de trabajo como instrumento a través del cual se canalizan las referentes necesidades de la industria relacionadas con la infraestructura de tecnologías de la información y como resultado actualizan los perfiles ocupacionales de la industria TI en siete líneas una de ellas soporte de infraestructura donde se encuentra el perfil del especialista en seguridad de la información.

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, Argentina, Chile y México.

<table>
<tr><th colspan="4">1. IDENTIFICACIÓN DE LA CUALIFICACIÓN</th></tr>
<tr><td colspan="2">Código de la cualificación: 6-INCO-ITS-008</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">Gestión de la seguridad de la información.</td></tr>
<tr><td>NIVEL DEL MNC</td><td colspan="3">6</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">20 a 32 créditos – 960 a 1536 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 especialista universitario.
(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, implementar, mantener y administrar el sistema de gestión de la seguridad de la información salvaguardando la integridad, confidencialidad y disponibilidad de la información respondiendo al cumplimiento de los objetivos organizacionales, la continuidad del negocio, aplicando metodologías, normativa técnica y jurídica en seguridad de la información.</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: sector primario y extractivo, comercio, industrial y servicios, públicas o privadas, productivas o de servicios. Desempeñándose en el área de soporte o administración de redes, manteniendo la continuidad operacional de los servicios que presta la red y los niveles de seguridad requeridos por el negocio. Principalmente en el sector de tecnologías de la información trabajando en conjunto con el administrador de la red.

Departamentos y empresas de sistemas e informática que requieren supervisar la ejecución de proyectos relacionados con la seguridad de redes informáticas multiservicio. Maneja su propia empresa prestando servicios o consultoría en sistemas de gestión de seguridad informática, 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 • Analista de seguridad de computadores. • Analista de seguridad de datos. • Analista de seguridad de las TIC. • Consultor de seguridad de datos. • Especialista en seguridad de información. • Especialista en seguridad de las TIC. • Auditor de sistemas. **Otras denominaciones:** • Director de seguridad de la información. • Analista en seguridad de la información. • Gestor de seguridad de la información. • Oficial de seguridad de la información.
COMPETENCIAS ESPECÍFICAS	**CE01-6-INCO-ITS-008-**Evaluar la seguridad de la información de la organización según procedimientos y normativa técnica.
	CE02-6-INCO-ITS-008-Planificar el sistema de gestión de seguridad de la información según procedimientos técnicos y normativos.
	CE03-6-INCO-ITS-008-Diseñar el sistema de gestión de la seguridad de la información de acuerdo con requisitos técnicos y normativa.
	CE04-6-INCO-ITS-008-Implementar el sistema de gestión de seguridad de la información de acuerdo con procedimientos y normativa técnica.
	CE05-6-INCO-ITS-008-Mantener el sistema de seguridad de la información acorde a procedimientos y normativa técnica.
	CE06-6-INCO-ITS-008-Administrar el sistema de gestión de seguridad de la información de acuerdo con metodología y políticas de continuidad del negocio.
COMPETENCIA ESPECIFICA	**CE01-6-INCO-ITS-008-**Evaluar la seguridad de la información de la organización según procedimientos y normativa técnica.
Elemento de competencia 1: Analizar el contexto organizacional y los requerimientos técnicos asociados a la seguridad de la información de acuerdo con normativa y criterios técnicos. **Criterios de desempeño:** • La revisión de la misión, visión y objetivos empresariales está conforme con buenas prácticas de referencia y normativa técnica. • El análisis de la estructura organizacional está conforme con el tipo de negocio. • La identificación de las necesidades en seguridad de la información cumple con requerimientos de la organización y criterios técnicos. • La identificación de requerimientos de seguridad a terceros está acorde con el tipo de negocio, normativa técnica y jurídica en seguridad de la información. • La revisión de normatividad jurídica en seguridad de la información está acorde con metodología de referencia y contexto organizacional. • La determinación del marco metodológico corresponde con las necesidades de la organización y referentes técnicos.	
Elemento de competencia 2: Diagnosticar el estado de la seguridad de la información de acuerdo con procedimientos y normativa técnica. **Criterios de desempeño:**	

- La evaluación de la política de seguridad de la información corresponde con procedimientos técnicos y metodología de referencia.
- El análisis del estado de la seguridad de la información corresponde con el contexto organizacional, normativa técnica y jurídica en seguridad de la información.
- La utilización de herramientas de diagnóstico en seguridad de la información cumple con procedimiento técnico y metodología de referencia.
- La valoración de la efectividad de los controles de seguridad cumple con procedimientos técnicos, normativa técnica y jurídica en seguridad de la información.
- La valoración de los controles de seguridad a terceros cumple con procedimientos técnicos y políticas de seguridad en la información.
- La identificación de acciones de mejora en la seguridad de la información está acorde con normatividad técnica y estrategia de continuidad del negocio.

Elemento de competencia 3: Precisar el alcance del sistema de gestión de seguridad de la información de acuerdo con requerimientos técnicos y los recursos de la organización.

Criterios de desempeño:

- La definición de los objetivos del sistema de seguridad de la información corresponde con el contexto y requerimientos organizacionales.
- La delimitación del alcance del sistema de gestión de seguridad de la información (SGSI) está acorde con los requerimientos técnicos y organizacionales.
- La definición de los procesos a impactar con el SGSI corresponde con políticas institucionales y estrategia de continuidad del negocio.
- La asignación de recursos a la protección de los activos de información está acorde con los objetivos y alcance del sistema de seguridad.
- El análisis de los riesgos asociados al proyecto está acorde con el estado actual de la seguridad en la organización.
- La determinación del marco metodológico corresponde con las necesidades de la organización y referentes técnicos.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, software de monitoreo de red, herramientas de diagnóstico en seguridad de la información.
- **Productos y resultados (evidencias):**
  Requerimientos en seguridad de la información.
  Documento de análisis del estado de la seguridad de la información de la organización.
  Objetivos y alcance del sistema de seguridad de la información.
  Lista de procesos a impactar con el SGSI.
  análisis de los riesgos asociados.
- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Requerimientos técnicos.
  Listado de asignación de recursos a la protección de los activos de la organización.
  Política de seguridad de la información.

COMPETENCIA ESPECIFICA	**CE02-6-INCO-ITS-008-**Planificar el sistema de gestión de seguridad de la información según procedimientos técnicos y normativos.

Elemento de competencia 1: Definir los activos de información según metodología técnica de referencia y procedimientos de la organización.

Criterios de desempeño:

- La identificación de los activos de información cumple con metodologías técnicas y requerimientos de la organización.
- El levantamiento del inventario de activos de información está acorde con procedimientos técnicos y metodología de referencia.
- La clasificación de activos de información está acorde con criterios técnicos y metodología de referencia.
- La valoración de los activos de información corresponde con la metodología de referencia y los objetivos de la seguridad de la información.
- La identificación de activos críticos de información para el negocio está acorde con procedimientos técnicos y metodologías de referencia.
- La consolidación de los activos de información corresponde con criterios técnicos de evaluación y metodología de referencia.

Elemento de competencia 2: Reconocer amenazas y vulnerabilidades sobre los activos de información de acuerdo con análisis técnico y metodología de referencia.

Criterios de desempeño:

- La identificación de amenazas está acorde con procedimientos técnicos y metodología de referencia.
- La utilización de herramientas de software para la detección de amenazas cumple con buenas prácticas de referencia y estándares técnicos.
- La valoración de la afectación de la amenaza sobre el activo de información está acorde con criterio técnico y metodología de referencia.
- La aplicación de herramientas de escaneo de vulnerabilidades está acorde con metodologías y procedimientos técnicos.
- La identificación de vulnerabilidades a partir del uso de herramientas de hacking ético está acorde con requerimientos organizacionales, normativa técnica y legal.
- La determinación de vulnerabilidades cumple con procedimientos técnicos y metodología de referencia.
- El registro de amenazas y vulnerabilidades está acorde con metodología de referencia.

Elemento de competencia 3: Establecer el análisis de riesgos de los activos de información según tipo de organización y metodología de referencia.

Criterios de desempeño:

- La determinación de los riesgos de seguridad está acorde con metodologías de análisis y criterios técnicos.
- La determinación 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 criterio técnico y metodología de referencia.
- La socialización del análisis de riesgos de seguridad de la información corresponde con los protocolos de la organización y criterio técnico.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, herramientas de software para la detección de amenazas, de hacking ético y de escaneo de vulnerabilidades.
- **Productos y resultados (evidencias):**
  Inventario de activos de información indicando los activos críticos de información para el negocio.
  Registrar amenazas y vulnerabilidades.
  Valorar el impacto de la materialización de los riesgos de seguridad.
  Socializar del análisis de riesgos de seguridad de la información.

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

COMPETENCIA ESPECIFICA	**CE03-6-INCO-ITS-008-**Diseñar el sistema de gestión de la seguridad de la información de acuerdo con requisitos técnicos y normativa.

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.

Criterios de desempeño:

- La verificación del cumplimiento de la legislación y normatividad asociada a 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 y las necesidades de la organización.
- La descripción del plan de tratamiento de riesgos cumple con referentes técnicos y normativa jurídica.
- 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.
- La elaboración 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: Estructurar 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.
- La definición 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 del incidente.
- 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: Construir 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, normativa técnica y jurídica en seguridad de la información.

- 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.
- **Productos y resultados (evidencias):**
  Cronograma de actividades para la implementación del SGSI.
  Plan de gestión de riesgos de seguridad de la información.
  Plan de gestión de incidentes de seguridad de la información.
  Documentar el programa de gestión de cambio, sensibilización y capacitación.
- **Información requerida (Referentes):**
  Documento que contenga la estrategia de continuidad del negocio.
  Normatividad técnica y jurídica en seguridad de la información.
  Requerimientos de seguridad de la información.
  Política de seguridad de la información y lineamientos organizacionales.

COMPETENCIA ESPECIFICA	**CE04-6-INCO-ITS-008**-Implementar el sistema de gestión de seguridad de la información de acuerdo con procedimientos y normativa técnica.

Elemento de competencia 1: Desplegar el sistema de gestión de seguridad de la información de acuerdo con normatividad técnica y requerimientos organizacionales.

Criterios de desempeño:

- La implantación de la política de seguridad de la información está acorde con lineamientos organizacionales y normatividad técnica.
- La aplicación de controles jurídicos cumple con normativa legal y técnica.
- La aplicación del plan de tratamiento y gestión de los riesgos de seguridad de la información cumple con procedimientos técnicos y organizacionales.
- El aseguramiento lógico y físico de la infraestructura TI está acorde con el plan de tratamiento y gestión de riesgos de seguridad de la información y procedimiento técnico.
- La configuración de los controles de seguridad en la infraestructura TI cumple con procedimiento y normativa técnica.
- La aplicación de técnicas criptográficas está acorde con el plan de tratamiento y gestión de riesgos de seguridad de la información y procedimiento técnico.
- La asignación de permisos sobre los recursos informáticos y activos de información está acorde con requerimientos organizacionales.
- La instalación y configuración de herramientas de monitorización está acorde con procedimiento técnico y requerimientos de la organización.

Elemento de competencia 2: Comprobar la efectividad del sistema de gestión de seguridad de la información de acuerdo con procedimientos y normativa técnica.

Criterios de desempeño:

- La aplicación de pruebas de penetración a redes e infraestructura TI cumple con normativa técnica y políticas organizacionales.
- La realización de auditorías de seguridad cumple con procedimientos y normativa técnica.
- La medición de la efectividad de la política de seguridad está acorde con procedimientos técnicos y organizacionales.

- La revisión de la funcionalidad de los controles de seguridad está acorde con procedimientos técnicos y metodología de referencia.
- La valoración de la efectividad de los controles de seguridad está acorde con metodología de referencia y criterios técnicos.
- La medición de la efectividad del plan de tratamiento de riesgos de seguridad de la información está acorde con metodologías y criterios técnicos.
- La valoración de la efectividad del sistema de gestión de seguridad de la información está acorde con diseño técnico y metodologías de referencia.

Elemento de competencia 3: Realizar las acciones de mejora del sistema de gestión de seguridad de la información de acuerdo con procedimientos técnicos y requerimientos de la organización.

Criterios de desempeño:

- La actualización de los controles jurídicos está acorde con la estrategia de continuidad del negocio y normativa legal.
- La actualización del inventario de activos de información cumple con metodología de referencia y procedimiento técnico.
- La reconfiguración de controles de seguridad en la infraestructura TI está acorde con los informes de auditoría de seguridad y procedimiento técnico.
- La determinación de acciones de mejora en el plan de tratamiento de riesgos de acuerdo con metodología e informe de auditoría de seguridad.
- El registro de hallazgos y actualización de la documentación cumple con metodología de referencia y requerimientos de la organización.

Elemento de competencia 4: Desarrollar los planes y programas de gestión de cambio y sensibilización en seguridad de la información de acuerdo con el SGSI y políticas de la organización.

Criterios de desempeño:

- La socialización de la política de seguridad de la información cumple con directrices gerenciales y procedimientos técnicos.
- La sensibilización de lineamientos y buenas prácticas de seguridad de la información están acorde con el SGSI y normativa técnica.
- La aplicación de los planes y programas de gestión de cambio y sensibilización en seguridad de la información cumple con políticas de la organización.
- La valoración de la efectividad de los planes de educación y sensibilización en seguridad de la información está acorde con metodologías de referencia.
- La medición del índice de cobertura de los planes de educación en seguridad de la información está acorde con normativa técnica.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, software de monitoreo.
- **Productos y resultados (evidencias):**
  Aplicar el plan de tratamiento y gestión de los riesgos.
  Configurar los controles de seguridad en la infraestructura TI.
  Aplicar pruebas de penetración a redes e infraestructura TI.
  Valorar de la efectividad de los controles de seguridad.
  Actualizar del inventario de activos de información.
  Registrar hallazgos y actualizar la documentación.
  Sensibilizar lineamientos y buenas prácticas de seguridad.
- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Política de seguridad de la información y lineamientos organizacionales.

Plan de educación en seguridad de la información.	
COMPETENCIA ESPECIFICA	**CE05-6-INCO-ITS-008-**Mantener el sistema de seguridad de la información acorde a procedimientos y normativa técnica.

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:

- El análisis del cumplimiento de las políticas de seguridad cumple con procedimientos técnicos y metodología.
- El análisis del tráfico de red está acorde con procedimiento técnico y organizacional.
- La identificación de amenazas y vulnerabilidades cumple con procedimiento técnico y metodología.
- El uso y manejo de las herramientas de monitoreo cumple con procedimientos técnicos y organizacionales.
- La recopilación de evidencias digitales está acorde con metodología y procedimientos organizacionales.
- La identificación de incidentes de seguridad de la información corresponde con procedimientos técnicos.
- La valoración de los mecanismos de seguridad está de acuerdo con metodología, normativa técnica y jurídica en seguridad de la información.
- El registro de eventos de seguridad corresponde con procedimiento técnico y políticas de la organización.

Elemento de competencia 2: Examinar los eventos e incidentes de seguridad de la información de acuerdo con procedimiento técnicos, organizacionales y normativa.

Criterios de desempeño:

- El reporte de eventos y debilidades en el sistema de seguridad de la información está acorde con procedimientos y metodología de referencia.
- La valoración del registro de eventos y logs cumple con normativa técnica y procedimientos de la organización.
- La correlación de eventos de seguridad cumple con normativa técnica y procedimientos de la organización.
- La detección de incidentes de seguridad cumple con procedimientos técnicos y organizacionales.
- La clasificación de incidentes de seguridad cumple con metodología de referencia y procedimientos de la organización.
- La determinación de la connotación de responsabilidad penal y civil del incidente de seguridad cumple con requerimientos de la organización y normativa legal.
- La evaluación de la efectividad de los controles está acorde con procedimiento técnico y SGSI.

Elemento de competencia 3: Gestionar los incidentes de seguridad de la información de acuerdo con procedimientos, normativa técnica y requerimientos de la organización.

Criterios de desempeño:

- La aplicación de acciones correctivas cumple con procedimientos técnicos y el plan de tratamiento de incidentes.
- La eliminación de la fuente de amenaza del incidente de seguridad está acorde con procedimientos y normativa técnica.
- El restablecimiento de los servicios afectados en el incidente de seguridad está acorde con procedimientos técnicos y estrategia de continuidad del negocio.
- La recuperación de incidentes de seguridad de la información está acorde con procedimientos técnicos y estrategia de continuidad del negocio.
- La definición de acciones preventivas y correctivas basados en los incidentes de seguridad cumple con metodología y requerimientos de la organización.
- La documentación del incidente de seguridad cumple con normativa técnica y procedimiento organizacional.
- La socialización del reporte del incidente de seguridad de la información está acorde con procedimientos organizacionales y metodología.

Elemento de competencia 4: Reforzar las competencias del talento humano relacionadas con seguridad de la información de acuerdo con políticas de la organización y plan de capacitación.

Criterios de desempeño:

- La medición de la efectividad del plan de gestión de cambio y capacitación está acorde con el plan de capacitación en seguridad de la información.
- El seguimiento al talento humano en la aplicación de habilidades en seguridad cumple con el plan de sensibilización y capacitación en seguridad.
- La actualización del plan de gestión de cambio y capacitación está acorde con las acciones de mejora y criterio técnico.
- La divulgación de campañas de generación de conciencia en seguridad cumple con políticas de la organización y plan de capacitación.
- El registro de las acciones de sensibilización y capacitación están acorde con los protocolos de la organización.
- La implementación de acciones de mejora está acorde con los reportes de satisfacción del usuario y necesidades del sistema de seguridad de la información.
- La aplicación de las acciones de mejora en planes de capacitación corresponde con la valoración de las capacitaciones y criterio técnico

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación, software de monitoreo.
- **Productos y resultados (evidencias):**
  Detectar y clasificar incidentes de seguridad de la información.
  Restablecer los servicios afectados en el incidente de seguridad.
  Definir acciones preventivas y correctivas basados en los incidentes de seguridad.
  Actualizar del plan de gestión de cambio y capacitación
- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Política de seguridad de la información y lineamientos organizacionales.
  Plan de capacitación en seguridad de la información.

COMPETENCIA ESPECIFICA	**CE06-6-INCO-ITS-008-**Administrar el sistema de gestión de seguridad de la información de acuerdo con metodología y políticas de continuidad del negocio.

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

Criterios de desempeño:

- La revisión de políticas y lineamientos de seguridad cumple con procedimiento técnico y organizacional.
- La evaluación de controles jurídicos está acorde con normativa legal y entorno del negocio.
- La valoración de la efectividad de los controles de seguridad está acorde con procedimientos técnicos y metodología de referencia.
- La aplicación de auditorías está acorde con procedimientos técnicos y metodología de referencia.
- La ejecución de pruebas de penetración al sistema cumple con normativa técnica y lineamientos organizacionales.
- La medición de la efectividad del sistema está acorde con procedimientos técnicos y metodología de referencia.
- La medición de efectividad del plan de gestión de incidentes está acorde con el plan de contención y recuperación de los incidentes de seguridad.
- La documentación de la auditoria de seguridad corresponde con procedimientos técnicos y políticas de la organización.
- La divulgación del informe de auditoría de seguridad cumple con procedimientos organizacionales y técnicos.

Elemento de competencia 2: Actualizar la información pertinente al sistema de gestión de seguridad de la información de acuerdo con metodología y políticas de continuidad del negocio.

Criterios de desempeño:

- La actualización del inventario de activos de información está acorde con la dinámica del negocio y políticas de la organización.
- La revisión de la calidad de la información consignada en el inventario de activos corresponde con procedimiento técnico y organizacional.
- La valoración de activos de información está acorde con procedimientos técnicos y metodología de referencia.
- La actualización de la valoración de riesgos de seguridad está acorde con procedimientos técnicos y metodología de referencia.
- La integración de las acciones de mejora al SGSI cumple con políticas de la organización y metodología de referencia.
- La actualización de los planes de continuidad y recuperación de incidentes de seguridad están acorde con normativas técnicas y estrategia del negocio.
- La actualización de los procedimientos documentados en el tratamiento de incidentes está acorde con la efectividad de los controles de seguridad.

Elemento de competencia 3: Mejorar el sistema de gestión de seguridad de la información de acuerdo con resultados de auditorías y políticas de continuidad del negocio.

Criterios de desempeño:

- La parametrización de los controles físicos o lógicos en el sistema de seguridad de la información cumple con procedimientos técnicos.
- La verificación de los controles en el sistema de seguridad de la información corresponde con criterio técnico y contexto normativo.
- La comprobación de la seguridad en la arquitectura de la red de datos cumple con criterio técnico y contexto normativo.
- La implementación de nuevos controles de seguridad está acorde con políticas de continuidad del negocio.
- La ejecución de las acciones preventivas y correctivas cumple con procedimientos técnicos.
- La documentación de las acciones de mejora al plan de gestión de riesgos corresponde con los hallazgos de la auditoria al sistema de seguridad de la información.

Elemento de competencia 4: Manejar los recursos del sistema de seguridad de la información de acuerdo con procedimientos administrativos y estrategia de continuidad del negocio.

Criterios de desempeño:

- La definición de indicadores de gestión y metodología de despliegue está acorde con los requerimientos de la organización.
- La coordinación de actividades del SGSI cumple con normativa técnica y requerimientos de la organización.
- La proyección de recursos para el SGSI está acorde con la estrategia de continuidad del negocio.
- La definición de roles, responsabilidades y recursos está acorde con metodología y requerimientos de la organización.
- La implementación del SGSI en la red de TI cumple con criterio técnico y política de la organización.
- El seguimiento al SGSI está acorde con requerimientos de la organización y metodología de referencia.
- La presentación de resultados a la gerencia cumple con políticas de la organización.

Contexto de la competencia

- **Recursos utilizados:** Computadores, software de aplicación.

- **Productos y resultados (evidencias):**
  Ejecutar pruebas de penetración.

Aplicar y documentar auditorias de seguridad de la información.
Implementar nuevos controles de seguridad.
Documentar las acciones de mejora al plan de gestión de riesgos.
Coordinar actividades del SGSI.
Implementar y realizar seguimiento del SGSI en la red de TI.

- **Información requerida (Referentes):**
  Normatividad técnica y jurídica en seguridad de la información.
  Política de seguridad de la información y lineamientos organizacionales.
  Políticas de continuidad del negocio.

COMPETENCIAS CLAVE (Básicas y transversales)

Competencias Básicas

Competencia	Duración
Comunicación y Solución de Problemas: • Medios de comunicación y otros sistemas simbólicos. • Ética de la comunicación. • 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 sentido de pertenencia en los miembros del equipo. • Gestión y aceptación de retos y desafíos. • Orientaciones para alcanzar metas y objetivos.	48 horas/ 1 crédito

	• Inspiración en los equipos de trabajo. • Buenas prácticas y mejores desempeños para lograr la calidad de vida laboral. • Generación y manejo del clima laboral positivo y armónico en un entorno de inclusión. • Comunicación asertiva en entornos de respeto • Situaciones y escenarios futuro-deseados en la organización.	
	Creatividad y Proactividad: • Comportamiento anticipatorio. • Presto al cambio tecnológico. • Autonomía. • Implementación de nuevos objetivos, formas de trabajo y procedimientos. • Estrategias de inspiración para la adaptación a las nuevas condiciones de trabajo. • Establece relaciones cordiales y reciprocas. • Manejo de contactos para obtener objetivos. • Generación de nuevas ideas y conceptos. • Ruptura de paradigmas en la solución de problemas. • Mente disruptiva. • Cocreatividad en la generación de nuevas ideas.	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. • Planes de acción para el desarrollo de los objetivos estratégicos. • Planeación organizacional con base en los indicadores y metas planeadas. • Planeación institucional con una visión estratégica acorde con necesidades y expectativas de usuarios. • Optimización los recursos. • Relación costo beneficio a corto, mediano y largo plazo.	48 horas/ 1 crédito
	Informática: • Herramientas ofimáticas • Manejo y uso de redes sociales • Aplicación de herramientas para producción de contenidos en redes sociales	48 horas/ 1 crédito
	Lógica de programación y Matemáticas: • Lógica proposicional.	

	• Lógica computacional. • Diagramación de flujos. • Lenguajes de hiper texto. • 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.	48 horas/ 1 crédito
	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. • 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.	48 horas/ 1 crédito

Competencias Transversales

Nombre de la Competencia Transversal		
Módulo	**Resultados de Aprendizaje**	**Duración**
Gestionar información a gran escala en tiempo razonable de acuerdo con infraestructuras, tecnologías y servicios disponibles	**RA1:** Clasifica grandes volúmenes de datos a partir de los criterios de procedencia y estructura. **RA2:** Aplica técnicas en la captura y recuperación de datos de acuerdo con necesidades de información. **RA3:** Identifica tendencias globales y patrones de los datos a partir de entornos de trabajo de datos masivos. **RA4:** Selecciona técnicas de almacenamiento de datos en función de la arquitectura del modelo de minería de datos.	48 horas/ 1 crédito

	Gestión del plan de protección ambiental	**RA1:** Formula acciones de mitigación de riesgos ambientales según el plan de protección ambiental de la organización. **RA2:** Selecciona estrategias de protección ambiental según los riesgos identificados y la normativa ambiental vigente. **RA3:** Establece mecanismos de seguimiento del plan de protección ambiental acorde con los lineamientos de la organización. **RA4:** Evalúa los riesgos derivados de su actividad, analizando las condiciones de trabajo y los factores de riesgo presentes en su entorno laboral.	48 horas/ 1 crédito
	Cultura emprendedora y empresarial Proponer ideas y buscar oportunidades	**RA1:** Aprovecha oportunidades que responden a retos y necesidades contrastando los intereses de los diferentes grupos de interés, experimentando y usando técnicas de aproximación y solución de problemas de manera creativa.	48 horas/ 1 crédito
	Cultura emprendedora y empresarial Manejar recursos	**RA2:** Inspira a otros a trabajar duro en sus objetivos y obtener juntos los recursos necesarios a partir de la actividad de creación de valor.	
	Cultura emprendedora y empresarial Educación financiera y económica	**RA3:** Construye indicadores financieros y emite concepto sobre el flujo de fondos requerido a partir de un proyecto complejo.	
	Cultura emprendedora y empresarial Pasar a la acción	**RA4:** Incorpora los objetivos de corto, mediano y largo plazo y redefine prioridades y planes de acción teniendo en cuenta las circunstancias cambiantes.	
	Cultura emprendedora y empresarial Manejar la incertidumbre, la ambigüedad y el riesgo	**RA5:** Compara las actividades de creación de valor basado en la evaluación de riesgos.	
	Innovación y desarrollo	**RA1:** Explica los principios y conceptos que sustentan los procedimientos, procesos, sistemas y metodologías de la profesión.	48 horas/ 1 crédito

		RA2: Aborda desde nuevos enfoques los problemas y/o necesidades, planteando soluciones y alternativas que generen valor, de acuerdo con criterios de viabilidad establecidos. **RA3:** Desarrolla procesos de mejoramiento de productos y servicios de su campo profesional de acuerdo con requerimientos definidos, oportunidades de mercado y metodologías de desarrollo de productos y servicios. **RA4:** Identifica y resuelve problemas en entornos nuevos o emergentes, de manera innovadora, dentro de contextos variados.	

3. REFERENTES PARA LA EDUCACIÓN Y FORMACIÓN	
CE01-6-INCO-ITS-008-Evaluar la seguridad de la información de la organización según procedimientos y normativa técnica.	
Duración créditos: 3 a 5	**Duración en horas: 144 a 240**
Resultado de aprendizaje 1. Interpretar la estructura y política organizacional de acuerdo con criterios técnicos y normativa.	
Resultado de aprendizaje 2. Determinar los requerimientos de seguridad de la información según criterios técnicos y normativa.	
Resultado de aprendizaje 3. Fijar el estado de la seguridad de la información de acuerdo con políticas de la organización	
Resultado de aprendizaje 4. Describir los lineamientos de mejora en la seguridad de la información según contexto normativo y jurídico.	
Resultado de aprendizaje 5. Contextualizar el sistema de gestión de seguridad de la información según las políticas de la organización	
Resultado de aprendizaje 6. Organizar los procesos, procedimientos y recursos que integran el sistema de gestión de seguridad de la información según las políticas de la organización	
CE02-6-INCO-ITS-008-Planificar el sistema de gestión de seguridad de la información según procedimientos técnicos y normativos.	
Duración créditos: 3 a 5	**Duración en horas: 144 a 240**
Resultado de aprendizaje 1. Disponer los inventarios de activos de la información de la organización de acuerdo con los criterios técnicos de la evaluación.	
Resultado de aprendizaje 2. Ubicar los activos críticos de información teniendo en cuenta los criterios técnicos y los objetivos del negocio.	
Resultado de aprendizaje 3. Detectar amenazas y vulnerabilidades del sistema de seguridad de la información de acuerdo con los criterios técnicos.	
Resultado de aprendizaje 4. Sistematizar las situaciones de amenaza y vulnerabilidad del sistema de seguridad de la información teniendo en cuenta los criterios técnicos y los objetivos del negocio.	
Resultado de aprendizaje 5. Caracterizar los riesgos de seguridad en el sistema de seguridad de la información según criterio técnico y métodos de análisis de riesgos.	

Resultado de aprendizaje 6. Dimensionar la ocurrencia del riesgo en el sistema de seguridad de la información de acuerdo con metodología de referencia y política de la organización.	
CE03-6-INCO-ITS-008-Diseñar el sistema de gestión de la seguridad de la información de acuerdo con requisitos técnicos y normativa.	
Duración créditos: 4 a 6	**Duración en horas: 192 a 288**
Resultado de aprendizaje 1. Seguir el cumplimiento normativo legal y tecnológico de la implementación del plan de gestión de riesgos en el sistema de la información según política organizacional.	
Resultado de aprendizaje 2. Documentar el plan de gestión de riesgos de seguridad de la información de acuerdo con metodologías y criterios técnicos.	
Resultado de aprendizaje 3. Proponer el plan de gestión de incidentes según criterio técnico y metodología de referencia.	
Resultado de aprendizaje 4. Instaurar el sistema de indicadores de efectividad del plan de gestión de incidentes de acuerdo con criterios técnicos.	
Resultado de aprendizaje 5. Programar las actividades de gestión de la seguridad de la información según políticas de la organización.	
Resultado de aprendizaje 6. Identificar necesidades de capacitación en seguridad de la información cumple con políticas de la organización	
CE04-6-INCO-ITS-008-Implementar el sistema de gestión de seguridad de la información de acuerdo con procedimientos y normativa técnica.	
Duración créditos: 4 a 6	**Duración en horas: 192 a 288**
Resultado de aprendizaje 1. Hacer los controles de seguridad en la infraestructura TI de acuerdo con el contexto normativo y legal de seguridad de la información.	
Resultado de aprendizaje 2. Configurar la arquitectura para el monitoreo de la seguridad de la infraestructura TI según criterio técnico y requerimientos de la organización.	
Resultado de aprendizaje 3. Controlar la efectividad del sistema de gestión de seguridad en redes e infraestructura TI de acuerdo con criterios técnicos.	
Resultado de aprendizaje 4. Supervisar la aplicación del control de seguridad en redes e infraestructura TI según metodología de referencia y criterios técnicos.	
Resultado de aprendizaje 5. Confirmar las condiciones de control y seguridad en la infraestructura TI según procedimiento y criterio técnico.	
Resultado de aprendizaje 6. Integrar acciones de mejora al sistema de seguridad en la infraestructura TI de acuerdo con el informe técnico de control.	
Resultado de aprendizaje 7. Diseñar programas de gestión de cambio y cultura de seguridad de la información teniendo en cuenta la política de la organización.	
Resultado de aprendizaje 8. Formular planes de capacitación de seguridad de la información de acuerdo con el contexto de la organización.	
CE05-6-INCO-ITS-008-Mantener el sistema de seguridad de la información acorde a procedimientos y normativa técnica.	
Duración créditos: 3 a 5	**Duración en horas: 144 a 240**
Resultado de aprendizaje 1. Observar el flujo y tráfico de la información en la red TI según criterios técnicos y políticas de la organización.	
Resultado de aprendizaje 2. Inspeccionar el sistema de seguridad de la información en la red TI según criterios técnicos y políticas de la organización.	
Resultado de aprendizaje 3. Utilizar técnicas de diagnóstico de eventos en el sistema de seguridad de acuerdo con criterio técnico y política de la organización.	
Resultado de aprendizaje 4. Correlacionar los eventos en el tráfico de la red con la normativa según criterio técnico y política de la organización.	
Resultado de aprendizaje 5. Atender requerimientos de mantenimiento en el sistema de seguridad de la información según criterio técnico.	

Resultado de aprendizaje 6. Detallar el manejo de situaciones de mantenimiento en el sistema de seguridad de la información según criterio técnico.
Resultado de aprendizaje 7. Apropiar nuevos enfoques en la gestión de cambio y capacitación del talento humano en sistemas de seguridad de la información de acuerdo con políticas de la organización.
Resultado de aprendizaje 8. Fomentar planes de mejora continua del talento humano en sistemas de seguridad de la información según políticas de la organización.
CE06-6-INCO-ITS-008-Administrar el sistema de gestión de seguridad de la información de acuerdo con metodología y políticas de continuidad del negocio.
Duración créditos: 3 a 5 | **Duración en horas: 144 a 240**
Resultado de aprendizaje 1. Difundir planes de control de la seguridad de acuerdo con criterio técnico y políticas de la organización.
Resultado de aprendizaje 2. Auditar el sistema de seguridad de la información teniendo en cuenta la política de la organización y criterio técnico.
Resultado de aprendizaje 3. Asegurar la calidad de los procesos de la gestión de la seguridad del flujo de información según criterio técnico y políticas de la organización.
Resultado de aprendizaje 4. Renovar las condiciones tecnológicas en la gestión de la seguridad del flujo de información de acuerdo con la normativa técnica.
Resultado de aprendizaje 5. Registrar los controles físicos o lógicos en el sistema de seguridad de la información según criterio y procedimiento técnico.
Resultado de aprendizaje 6. Generar estrategias de buenas prácticas en el manejo del sistema de seguridad de la información de acuerdo con las políticas de la organización.
Resultado de aprendizaje 7. Dirigir el desarrollo de las actividades del sistema de gestión de seguridad de la información en la red de TI teniendo en cuenta criterio técnico y política de la organización.
Resultado de aprendizaje 8. Chequear la ejecución del sistema de gestión de seguridad de la información en la red de TI según criterio técnico y política de la organización.

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.