1. APLICACIÓN DEL ANÁLISIS FUNCIONAL DE LA FIGURA PROFESIONAL "SEGURIDAD INFORMÁTICA"

El análisis funcional (AF) constituye una técnica metodológica orientada para identificar, organizar y estructurar las actividades de un proceso productivo o de prestación de servicios. Representa el punto de partida para elaborar el perfil profesional en términos de competencias y la base para el diseño curricular. En este marco, se presentan los elementos que integran el análisis funcional aplicados a la figura profesional de "Seguridad Informática".

a) Identificación del Objetivo:

La Seguridad Informática busca garantizar la confidencialidad, integridad y disponibilidad de la información, promoviendo entornos digitales seguros. Permite formar bachilleres técnicos capaces de proteger la información digital y los sistemas tecnológicos de una organización, mediante la identificación de riesgos, la implementación de mecanismos de protección de datos, el monitoreo continuo de la infraestructura tecnológica y la aplicación de normativas de seguridad vigentes y principios éticos en cumplimiento con estándares nacionales e internacionales.

b) Deducción de las actividades profesionales

- Gestión de la Seguridad de la Información
- Monitoreo y respuestas a incidentes en la seguridad de la información
- Administración de infraestructura segura
- Técnicas para proteger los flujos de información
- Evaluar y tratar los riesgos de seguridad
- Cumplimiento legal y normativo

Además de su base de conocimientos, estos bachilleres poseen cualidades esenciales como la ética, el liderazgo, habilidades de comunicación y en la resolución de problemas. Están siempre orientados a proporcionar un servicio de alta calidad y están preparados para enfrentar con éxito las cambiantes tendencias del mercado, tanto a nivel nacional como internacional.

c) Desagregación de las actividades

A continuación, se desagregan las actividades profesionales que se encuentran en el campo de la Seguridad Informática:

- Gestión de la Seguridad de la Información
  - Realizar procedimientos de seguridad de la información
  - Establecer mecanismos de clasificación de la información
  - Aplicar controles administrativos, físicos y técnicos para proteger y mitigar riesgos en la infraestructura tecnológica.
  - Gestionar respaldos y planes de continuidad de la organización
- Monitoreo y respuestas a Incidentes en la seguridad de la información
  - Implementar herramientas de monitoreo de red
  - Analizar registros de eventos y detectar actividades sospechosas

  - Responder ante incidentes siguiendo protocolos establecidos
  - Documentar incidentes y elaborar informes post-incidentes.
- Administración de infraestructura segura
  - Configurar redes seguras
  - Gestionar permisos, roles y accesos de usuarios
  - Instalar y mantener sistemas de protección en servidores y estaciones de trabajo, aplicando técnicas de hardening.
- Técnicas para proteger los flujos de información
  - Emplear protocolos seguros
  - Asegurar la integridad de los datos mediante funciones hash
  - Utilizar mecanismos de autenticación multifactor (MFA)
- Evaluar y tratar los riesgos de seguridad
  - Identificar amenazas y vulnerabilidad en la infraestructura tecnológica
  - Estimar impacto y probabilidad del riesgo
  - Proponer e implementar controles para mitigar riesgos
  - Evaluar la seguridad de la información mediante técnicas hacking ético.
  - Documentar planes de tratamiento de riesgos y seguimiento de su efectividad
- Cumplimiento legal y normativo
  - Interpretar y aplicar normativas como LOPDP (Ecuador), ISO/IEC 27001, NIST
  - Verificar el cumplimiento de políticas internas y legales
  - Generar reportes de cumplimiento y control de evidencias

Además de sus competencias técnicas en protección de la información, gestión de riesgos, implementación de mecanismos de seguridad y administración de sistemas, las y los estudiantes fortalecen cualidades esenciales como el liderazgo, la comunicación efectiva y la capacidad para resolver problemas. Se distinguen por su compromiso con la calidad en la gestión de entornos digitales seguros y por estar preparados para adaptarse con éxito a los constantes cambios y exigencias del entorno tecnológico y del mercado laboral en el área de la seguridad informática.

2. PERFIL PROFESIONAL DE LA FIGURA “SEGURIDAD INFORMÁTICA”

1. Caracterización

La Seguridad Informática es una especialización técnica que busca garantizar la confidencialidad, integridad y disponibilidad de la información, promoviendo entornos digitales seguros. Permite formar bachilleres técnicos capaces de proteger la información digital y los sistemas tecnológicos de una organización, mediante la identificación de riesgos, la implementación de mecanismos de protección de datos, el monitoreo continuo de la infraestructura tecnológica y la aplicación de normativas de seguridad vigentes y principios éticos en cumplimiento con estándares nacionales e internacionales.

2. Definición

Al egresar, la/el Bachiller técnico en Seguridad Informática; es capaz de aplicar técnicas de manejo de datos y soluciones informáticas que le permitirán identificar vulnerabilidades en

sistemas y redes, así como para implementar estrategias orientadas a la prevención, detección y respuesta ante amenazas. Su formación contribuirá activamente a garantizar la confidencialidad, integridad y disponibilidad de la información, elementos fundamentales para la protección de los entornos digitales en diversos sectores.

Aspectos destacados del perfil profesional

- **Conocimiento Técnico-Científico:** Tendrán una comprensión e integración de principios científicos y tecnológicos relacionados con la seguridad informática, sustentando sus decisiones y acciones en fundamentos técnicos, metodológicos y éticos.
- **Habilidades Comunicativas:** Desarrollarán habilidades que les permitan comunicarse con claridad, liderazgo y empatía, en la atención de incidentes de forma asertiva y resolución de conflictos relacionados con la gestión de la seguridad y la información.
- **Liderazgo y Trabajo en Equipo:** Demostrarán habilidades para trabajar de manera efectiva con usuarios, proveedores de servicios tecnológicos y personal de soporte, con responsabilidad, iniciativa, fomentando un ambiente colaborativo que permita prevenir, detectar y responder de forma oportuna a incidentes de seguridad.
- **Pensamiento crítico y analítico:** Tendrán capacidad para analizar problemas de seguridad desde distintas perspectivas, evaluando causas y soluciones con criterio técnico y ético.

3. Campo ocupacional

El campo ocupacional que las y los estudiantes del Bachillerato Técnico de Seguridad Informática podrán insertarse son los siguientes:

- **Ocupaciones y puestos de trabajo relacionados**
  - Asistente en Seguridad Informática.
  - Soporte técnico con enfoque en Seguridad
  - Auxiliar técnico/a en implementación de seguridades en sistemas informáticos.
  - Operador/a de seguridad de redes.
  - Auxiliar técnico/a en gestión de incidentes.
  - Instalador/a de Sistemas de Seguridad Informática.
  - Auxiliar Técnico/a en Respaldo y recuperación de información.
  - Sectores productivos y organizaciones

- **Sectores productivos y organizaciones**

El/la Bachiller Técnico en Seguridad Informática podrá trabajar en:

  - Departamentos de tecnologías en instituciones públicas y privadas.
  - Empresas proveedoras de servicios informáticos o de seguridad.
  - Centros de datos, redes empresariales y entorno de nube.

- Proyecto de desarrollo y soporte informático.
- Centros de seguridad informática de empresas especializadas.
- Equipos de respuesta a incidentes de ciberseguridad.
- Instituciones educativas, bancarias, de salud, cooperativas, financieras, operadoras de comunicación, farmacéuticas, instituciones militares.

4. Competencia general

Gestionar la protección de la información digital y la seguridad de los sistemas informáticos, mediante el diseño, implementación y monitoreo de medidas de prevención, detección y respuesta ante amenazas, aplicando tecnologías, herramientas, normativas y protocolos que garanticen la confidencialidad, integridad y disponibilidad de los activos en distintos entornos organizacionales.

4.1. Unidades de competencia

UNIDAD DE COMPETENCIA (UC)	
UC 1: Analizar el estado de seguridad y vulnerabilidades de la red y de los sistemas informáticos, con el fin de reducir amenazas y proponer soluciones digitales.	
Elementos de competencia (EC)	**Criterios de desempeño (CD)**
EC1: Seleccionar los activos informáticos que contengan información crítica, aplicando principios de seguridad de la información.	CD1.1: Distingue los activos clave (hardware, software, datos, servicios) considerando su valor para la organización.
	CD1.2: Clasifica los activos según su importancia en la confidencialidad, integridad y disponibilidad de la información.
	CD1.3: Analiza principios básicos de riesgos en la priorización de los activos con base en su impacto potencial frente a amenazas.
	CD1.4: Cataloga los activos identificados en un inventario básico, incluyendo su ubicación, tipo de información que manejan y criticidad.
EC2: Distinguir las amenazas potenciales internas y externas que pueden afectar los sistemas informáticos utilizando marcos de referencia para su clasificación.	CD2.1: Diferencia correctamente amenazas internas como accesos indebidos, errores de configuración, negligencia o sabotaje.
	CD2.2: Compara amenazas externas como malware, phishing, ransomware, ataques por fuerza bruta, entre otros.
	CD2.3: Relaciona amenazas con vulnerabilidades, evaluando su impacto en la confidencialidad, integridad y disponibilidad.
	CD2.4: Utiliza las listas y marcos de referencia simplificados (como OWASP Top 10) para describir tipos comunes de amenazas.
	CD3.1: Usa herramientas accesibles y seguras para identificar configuraciones inseguras o servicios expuestos.
	CD3.2: Aplica técnicas básicas de escaneo en entornos de laboratorio o simulación, respetando políticas de no intrusión.

EC3: Detectar vulnerabilidades y brechas de seguridad utilizando herramientas básicas, interpretando los resultados y proponiendo acciones de mitigación.	CD3.3: Interpreta los resultados de las herramientas, diferenciando falsos positivos y priorizando hallazgos por criticidad.
	CD3.4: Propone acciones básicas de corrección o mitigación en base a buenas prácticas y al entorno evaluado.
EC4: Justificar los hallazgos de seguridad en un informe técnico con lenguaje adecuado, respetando estándares de manejo seguro de la información.	CD4.1: Organiza la información recolectada de manera estructurada, siguiendo un formato prediseñado.
	CD4.2: Elabora informes con lenguaje técnico claro y adecuado al contexto educativo o institucional.
	CD4.3: Presenta el informe aplicando principios básicos de manejo seguro de la información (confidencialidad, integridad y trazabilidad).
Condiciones de ejecución de la Unidad de Competencia:	
Espacios e instalaciones:	Entorno de aprendizaje Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización. Acceso a laboratorio virtual (local o en la nube) para simulaciones controladas.
Insumos y recursos:	**Sistemas Operativos (mínimos requeridos y recomendados):** • Windows 10 u 11 (mínimo requerido) • Ubuntu Desktop (mínimo requerido) • Kali Linux (mínimo requerido) • Parrot OS (recomendado para prácticas ofensivas) • Rocky Linux o CentOS Stream (recomendado para administración de servidores) **Virtualización y entornos controlados:**

	• VirtualBox (mínimo requerido) • VMware Workstation o Player (mínimo requerido) • Hyper-V (recomendado) • VMware ESXi (recomendado para prácticas avanzadas o institucionales) **Conectividad:** • Internet de alta velocidad (mínimo requerido) • Red interna aislada para simulacros y ejercicios de ciberseguridad • Herramientas de Seguridad y Análisis **Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Laboratorios virtuales y simuladores:** • Máquinas virtuales locales (VirtualBox o VMware) • TryHackMe (recomendado) • VulnHub (recomendado)

	• OWASP Juice Shop (recomendado para prácticas de seguridad web) • Cyber Range local o institucional (recomendado) **Plataformas Educativas y de Apoyo Didáctico** • Moodle o Google Classroom (mínimo requerido) • draw.io o similares para diagramación técnica (recomendado) • LibreOffice o software ofimático compatible (mínimo requerido) • Trello o herramienta tipo Kanban (recomendado para gestión de tareas) • Herramientas de Monitoreo y Gestión de Incidentes **Monitoreo de redes y sistemas:** • Nagios (recomendado) • Zabbix (recomendado) • Grafana (recomendado) **Gestión de tickets e incidentes:** • GLPI o OTRS (recomendado) **Sistemas de detección y análisis:** • Consolas básicas de Snort (mínimo requerido) • Suricata integrado con Kibana o ELK Stack (recomendado) **Hardware complementario:** • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado)

	• Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)
Información utilizada:	Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible) NIST SP 800-30 (análisis de riesgos) NIST SP 800-53 (controles de seguridad para sistemas de información) ISO/IEC 27001 (gestión de la seguridad de la información) ISO/IEC 27002 (controles de seguridad) OWASP Top 10 (riesgos en aplicaciones web) MITRE ATT&CK (catálogo de técnicas y tácticas de ataque) Ley Orgánica de Protección de Datos Personales (LOPDP) Código Orgánico Integral Penal (COIP), sección delitos informáticos Ley de Comercio Electrónico, Firmas y Mensajes de Datos Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles) CIS Benchmarks para hardening de sistemas Guías de configuración segura de NIST Manuales institucionales o académicos para Windows/Linux Manuales y documentación de herramientas como Nmap, Nessus, Metasploit, Snort, Suricata, Wireshark, Hashcat, John the Ripper Guías de configuración básica de firewalls y routers Modelos de informes técnicos de vulnerabilidades Plantillas de inventario de activos y matrices de criticidad Listados de usuarios, accesos y permisos simulados Informes de amenazas regionales (por ejemplo, ESET, Fortinet, Kaspersky)

	Política de uso aceptable Política de control de accesos Política de respaldo y recuperación Política de manejo de incidentes de seguridad

UNIDAD DE COMPETENCIA (UC)	
UC 2: Aplicar protocolos de respuesta ante incidentes, recuperando sistemas y respaldos de información, garantizando la continuidad operativa de los servicios.	
Elementos de competencia (EC)	**Criterios de desempeño (CD)**
EC1: Clasificar los tipos de incidentes de seguridad informática distinguiendo eventos y aplicando las etapas del ciclo de respuesta.	CD1.1: Distingue eventos de seguridad como errores humanos, fallos técnicos, accesos no autorizados o ataques maliciosos.
	CD1.2: Clasifica los incidentes por origen (interno/externo), tipo (tecnológico/humano) e intencionalidad (accidental/deliberado), utilizando categorías simplificadas.
	CD1.3: Aplica las etapas básicas del ciclo de respuesta ante incidentes: detección, análisis, contención, erradicación y recuperación.
EC2: Establecer acciones básicas de contención y mitigación frente a incidentes utilizando procedimientos controlados y registrando la trazabilidad de las acciones ejecutadas.	CD 2.1: Usa comandos, herramientas o procedimientos básicos (como deshabilitación de servicios, aislamiento de red o uso de antivirus) en entornos controlados.
	CD2.2: Justifica la decisión de aislar sistemas comprometidos evitando la propagación del incidente, según protocolos preestablecidos en prácticas simuladas.

	CD2.3: Cataloga las acciones ejecutadas utilizando una bitácora técnica clara, manteniendo trazabilidad de los pasos tomados.
EC3: Restaurar los sistemas afectados utilizando respaldos verificados y validación funcional.	CD3.1: Verifica que las copias de respaldo estén completas y sin alteraciones antes de restaurar datos.
	CD3.2: Evalúa el nivel de daño sufrido por los sistemas y selecciona el método de restauración más apropiado.
	CD3.3: Restaura correctamente sistemas operativos, configuraciones o archivos desde copias de seguridad locales o en la nube.
	CD3.4: Realiza pruebas de funcionalidad básicas (servicios activos, accesos permitidos, ausencia de errores) para validar la correcta recuperación del sistema.
Condiciones de ejecución de la Unidad de Competencia:	
Espacios e instalaciones:	Entorno de aprendizaje Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización. Acceso a laboratorio virtual (local o en la nube) para simulaciones controladas.
Insumos y recursos:	**Sistemas Operativos (mínimos requeridos y recomendados):** • Windows 10 u 11 (mínimo requerido) • Ubuntu Desktop (mínimo requerido) • Kali Linux (mínimo requerido) • Parrot OS (recomendado para prácticas ofensivas)

	• Rocky Linux o CentOS Stream (recomendado para administración de servidores) **Virtualización y entornos controlados:** • VirtualBox (mínimo requerido) • VMware Workstation o Player (mínimo requerido) • Hyper-V (recomendado) • VMware ESXi (recomendado para prácticas avanzadas o institucionales) **Conectividad:** • Internet de alta velocidad (mínimo requerido) • Red interna aislada para simulacros y ejercicios de ciberseguridad • Herramientas de Seguridad y Análisis **Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Laboratorios virtuales y simuladores:**

	• Máquinas virtuales locales (VirtualBox o VMware) • TryHackMe (recomendado) • VulnHub (recomendado) • OWASP Juice Shop (recomendado para prácticas de seguridad web) • Cyber Range local o institucional (recomendado) **Plataformas Educativas y de Apoyo Didáctico:** • Moodle o Google Classroom (mínimo requerido) • draw.io o similares para diagramación técnica (recomendado) • LibreOffice o software ofimático compatible (mínimo requerido) • Trello o herramienta tipo Kanban (recomendado para gestión de tareas) • Herramientas de Monitoreo y Gestión de Incidentes **Monitoreo de redes y sistemas:** • Nagios (recomendado) • Zabbix (recomendado) • Grafana (recomendado) **Gestión de tickets e incidentes:** • GLPI o OTRS (recomendado) **Sistemas de detección y análisis:** • Consolas básicas de Snort (mínimo requerido) • Suricata integrado con Kibana o ELK Stack (recomendado)

	Hardware complementario: • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado) • Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)
Información utilizada:	Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible) NIST SP 800-30 (análisis de riesgos) NIST SP 800-53 (controles de seguridad para sistemas de información) ISO/IEC 27001 (gestión de la seguridad de la información) ISO/IEC 27002 (controles de seguridad) OWASP Top 10 (riesgos en aplicaciones web) MITRE ATT&CK (catálogo de técnicas y tácticas de ataque) Ley Orgánica de Protección de Datos Personales (LOPDP) Código Orgánico Integral Penal (COIP), sección delitos informáticos Ley de Comercio Electrónico, Firmas y Mensajes de Datos Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles) CIS Benchmarks para hardening de sistemas Guías de configuración segura de NIST Manuales institucionales o académicos para Windows/Linux Manuales y documentación de herramientas como Nmap, Nessus, Metasploit, Snort, Suricata, Wireshark, Hashcat, John the Ripper Guías de configuración básica de firewalls y routers Modelos de informes técnicos de vulnerabilidades

	Plantillas de inventario de activos y matrices de criticidad Listados de usuarios, accesos y permisos simulados Informes de amenazas regionales (por ejemplo, ESET, Fortinet, Kaspersky) Política de uso aceptable Política de control de accesos Política de respaldo y recuperación Política de manejo de incidentes de seguridad

UNIDAD DE COMPETENCIA (UC)	
UC 3: Realizar el monitoreo de redes y sistemas informáticos en forma periódica en la detección de eventos de seguridad y riesgos, aplicando herramientas de supervisión, análisis de datos y elaboración de reportes técnicos conforme a protocolos establecidos, con el fin de mantener la disponibilidad y confiabilidad de los servicios.	
Elementos de competencia (EC)	**Criterios de desempeño (CD)**
EC1: Analizar los datos recolectados en la evaluación de riesgos y posibles incidentes correlacionando eventos y priorizando alertas según su criticidad.	CD1.1: Examina de forma sistemática los datos recolectados por las herramientas de monitoreo, prestando atención a patrones inusuales.
	CD1.2: Distingue entre eventos normales y señales de amenazas o incidentes en curso.
	CD1.3: Establece relaciones entre eventos múltiples para detectar posibles ataques encadenados (por ejemplo, escaneo + acceso + escalamiento).
	CD1.4: Prioriza las alertas según nivel de criticidad, contexto del activo comprometido y probabilidad de ocurrencia.
EC2: Emplear herramientas y procedimientos de monitoreo continuo en redes y sistemas,	CD2.1: Usa herramientas básicas de monitoreo (como Wazuh, Zabbix, Nagios o similares) para la supervisión continua de servicios, puertos, autenticaciones y tráfico.

definiendo parámetros de supervisión y clasificando eventos según relevancia técnica.	CD2.2: Define parámetros de operación normal y establece umbrales de alerta para detectar desviaciones o anomalías.
	CD2.3: Distingue que los registros del monitoreo incluyan eventos clave como inicios de sesión, cambios de configuración, accesos sospechosos y uso de recursos.
	CD2.4: Garantiza la integridad, disponibilidad y confidencialidad de los registros generados por el monitoreo.
EC3: Descubrir eventos de seguridad o comportamientos inusuales en los sistemas monitoreados utilizando herramientas de detección para su interpretación y seguimiento según procedimientos establecidos.	CD3.1: Distingue comportamientos anómalos como picos de tráfico, accesos no autorizados o modificaciones inesperadas en archivos o configuraciones.
	CD3.2: Clasifica los eventos detectados de acuerdo con su severidad, impacto potencial y urgencia de respuesta.
	CD3.3: Utiliza herramientas de detección de intrusos (IDS) y análisis de logs para interpretar los eventos de seguridad capturados.
	CD3.4: Clasifica los eventos detectados, conforme a procedimientos establecidos para su evaluación y seguimiento.
EC4: Elaborar reportes técnicos con hallazgos evidencias y recomendaciones de mejora, organizándolos de forma estructurada y asegurando su trazabilidad, integridad y confidencialidad.	CD4.1: Construye reportes técnicos con los hallazgos del monitoreo, incluyendo descripciones, evidencias y análisis técnico.
	CD4.2: Organiza los reportes de forma estructurada, considerando el perfil técnico o administrativo del destinatario.
	CD4.3: Propone recomendaciones prácticas para ajustar configuraciones o reforzar el sistema de monitoreo.
	CD4.4: Clasifica los reportes siguiendo principios de trazabilidad, integridad de datos y confidencialidad.
Condiciones de ejecución de la Unidad de Competencia:	
Espacios e instalaciones:	Entorno de aprendizaje

	Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización. Acceso a laboratorio virtual (local o en la nube) para simulaciones controladas.
Insumos y recursos:	**Sistemas Operativos (mínimos requeridos y recomendados):** • Windows 10 u 11 (mínimo requerido) • Ubuntu Desktop (mínimo requerido) • Kali Linux (mínimo requerido) • Parrot OS (recomendado para prácticas ofensivas) • Rocky Linux o CentOS Stream (recomendado para administración de servidores) **Virtualización y entornos controlados:** • VirtualBox (mínimo requerido) • VMware Workstation o Player (mínimo requerido) • Hyper-V (recomendado) • VMware ESXi (recomendado para prácticas avanzadas o institucionales) **Conectividad:** • Internet de alta velocidad (mínimo requerido) • Red interna aislada para simulacros y ejercicios de ciberseguridad • Herramientas de Seguridad y Análisis **Herramientas de diagnóstico y análisis:** • Nmap

	• OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Laboratorios virtuales y simuladores:** • Máquinas virtuales locales (VirtualBox o VMware) • TryHackMe (recomendado) • VulnHub (recomendado) • OWASP Juice Shop (recomendado para prácticas de seguridad web) • Cyber Range local o institucional (recomendado) **Plataformas Educativas y de Apoyo Didáctico** • Moodle o Google Classroom (mínimo requerido) • draw.io o similares para diagramación técnica (recomendado) • LibreOffice o software ofimático compatible (mínimo requerido) • Trello o herramienta tipo Kanban (recomendado para gestión de tareas) • Herramientas de Monitoreo y Gestión de Incidentes **Monitoreo de redes y sistemas:**

	• Nagios (recomendado) • Zabbix (recomendado) • Grafana (recomendado) **Gestión de tickets e incidentes:** • GLPI o OTRS (recomendado) **Sistemas de detección y análisis:** • Consolas básicas de Snort (mínimo requerido) • Suricata integrado con Kibana o ELK Stack (recomendado) **Hardware complementario:** • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado) Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)
Información utilizada:	Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible) NIST SP 800-30 (análisis de riesgos) NIST SP 800-53 (controles de seguridad para sistemas de información) ISO/IEC 27001 (gestión de la seguridad de la información) ISO/IEC 27002 (controles de seguridad) OWASP Top 10 (riesgos en aplicaciones web) MITRE ATT&CK (catálogo de técnicas y tácticas de ataque) Ley Orgánica de Protección de Datos Personales (LOPDP) Código Orgánico Integral Penal (COIP), sección delitos informáticos Ley de Comercio Electrónico, Firmas y Mensajes de Datos

	Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles) CIS Benchmarks para hardening de sistemas Guías de configuración segura de NIST Manuales institucionales o académicos para Windows/Linux Manuales y documentación de herramientas como Nmap, Nessus, Metasploit, Snort, Suricata, Wireshark, Hashcat, John the Ripper Guías de configuración básica de firewalls y routers Modelos de informes técnicos de vulnerabilidades Plantillas de inventario de activos y matrices de criticidad Listados de usuarios, accesos y permisos simulados Informes de amenazas regionales (por ejemplo, ESET, Fortinet, Kaspersky) Política de uso aceptable Política de control de accesos Política de respaldo y recuperación Política de manejo de incidentes de seguridad

UNIDAD DE COMPETENCIA (UC)	
UC 4: Emplear normas de protección de datos y de ciberseguridad en sistemas informáticos, garantizando la protección de información sensible.	
Elementos de competencia (EC)	**Criterios de desempeño (CD)**
EC1: Clasificar las principales normas, leyes y marcos regulatorios aplicables a la protección de datos y ciberseguridad, interpretando sus principios y relacionándolos con situaciones prácticas.	CD1.1: Cataloga las principales leyes y normas relacionadas con la protección de datos y la ciberseguridad, como la LOPDP y el COIP en Ecuador, e instrumentos internacionales como el RGPD e ISO/IEC 27001.

	CD1.2: Explica las consecuencias legales, técnicas y organizacionales del incumplimiento de normas sobre protección de datos.
	CD1.3: Aplica los principios fundamentales de la protección de datos, tales como consentimiento informado, minimización, finalidad, seguridad y responsabilidad.
	CD1.4: Relaciona correctamente marcos normativos con situaciones comunes en entornos educativos, laborales o comunitarios.
EC2: Analizar los principios de protección de datos con la seguridad de la información, evaluando riesgos y proponiendo medidas para proteger datos sensibles.	CD2.1: Analiza cómo se aplican los principios de protección de datos personales en casos reales o simulados de manejo de información.
	CD2.2: Relaciona los principios de protección de datos con los pilares de la seguridad de la información: confidencialidad, integridad, disponibilidad y trazabilidad.
	CD2.3: Examina los riesgos y consecuencias de no aplicar los principios de protección de datos sobre los titulares de la información.
	CD2.4: Propone medidas básicas como encriptación, control de accesos, respaldos o anonimización, para proteger datos sensibles.
EC3: Aplicar políticas organizacionales y controles técnicos conforme a normas y estándares básicos de seguridad, configurando parámetros adecuados y realizando mejoras ante debilidades detectadas.	CD3.1: Utiliza controles técnicos como autenticación, cifrado, respaldo y bitácoras, alineados con políticas organizacionales de seguridad.
	CD3.2: Configura parámetros de seguridad adecuados para proteger el acceso y la integridad de los datos, en plataformas o entornos simulados.
	CD3.3: Evalúa de forma general la eficacia de los controles frente a amenazas comunes.
	CD3.4: Realiza mejoras prácticas ante debilidades o incumplimientos detectados en los controles aplicados.

EC4: Relacionar los controles de seguridad con los requisitos establecidos en normas de referencia, identificando tipos, utilizando mapeos y considerando el marco legal aplicable.	CD4.1: Analiza los tipos de controles de seguridad: preventivos, detectivos y correctivos, sus aplicaciones en la protección de sistemas y datos.
	CD4.2: Utiliza herramientas o esquemas de mapeo normativo básico para verificar el cumplimiento de requisitos.
	CD4.3: Demuestra comprensión del marco legal nacional e internacional y su importancia en la gestión de la seguridad de la información.
	CD4.4: Integra controles comunes con estándares como ISO/IEC 27001 o NIST CSF, en forma general y aplicada al contexto nacional.
Condiciones de ejecución de la Unidad de Competencia:	
Espacios e instalaciones:	Entorno de aprendizaje Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización. Acceso a laboratorio virtual (local o en la nube) para simulaciones controladas.
Insumos y recursos:	**Sistemas Operativos (mínimos requeridos y recomendados):** • Windows 10 u 11 (mínimo requerido) • Ubuntu Desktop (mínimo requerido) • Kali Linux (mínimo requerido) • Parrot OS (recomendado para prácticas ofensivas) • Rocky Linux o CentOS Stream (recomendado para administración de servidores) **Virtualización y entornos controlados:**

	• VirtualBox (mínimo requerido) • VMware Workstation o Player (mínimo requerido) • Hyper-V (recomendado) • VMware ESXi (recomendado para prácticas avanzadas o institucionales) **Conectividad:** • Internet de alta velocidad (mínimo requerido) • Red interna aislada para simulacros y ejercicios de ciberseguridad • Herramientas de Seguridad y Análisis **Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Laboratorios virtuales y simuladores:** • Máquinas virtuales locales (VirtualBox o VMware) • TryHackMe (recomendado) • VulnHub (recomendado)

	• OWASP Juice Shop (recomendado para prácticas de seguridad web) • Cyber Range local o institucional (recomendado) **Plataformas Educativas y de Apoyo Didáctico** • Moodle o Google Classroom (mínimo requerido) • draw.io o similares para diagramación técnica (recomendado) • LibreOffice o software ofimático compatible (mínimo requerido) • Trello o herramienta tipo Kanban (recomendado para gestión de tareas) • Herramientas de Monitoreo y Gestión de Incidentes **Monitoreo de redes y sistemas:** • Nagios (recomendado) • Zabbix (recomendado) • Grafana (recomendado) **Gestión de tickets e incidentes:** • GLPI o OTRS (recomendado) **Sistemas de detección y análisis:** • Consolas básicas de Snort (mínimo requerido) • Suricata integrado con Kibana o ELK Stack (recomendado) **Hardware complementario:** • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado)

	Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)
Información utilizada:	Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible) NIST SP 800-30 (análisis de riesgos) NIST SP 800-53 (controles de seguridad para sistemas de información) ISO/IEC 27001 (gestión de la seguridad de la información) ISO/IEC 27002 (controles de seguridad) OWASP Top 10 (riesgos en aplicaciones web) MITRE ATT&CK (catálogo de técnicas y tácticas de ataque) Ley Orgánica de Protección de Datos Personales (LOPDP) Código Orgánico Integral Penal (COIP), sección delitos informáticos Ley de Comercio Electrónico, Firmas y Mensajes de Datos Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles) CIS Benchmarks para hardening de sistemas Guías de configuración segura de NIST Manuales institucionales o académicos para Windows/Linux Manuales y documentación de herramientas como Nmap, Nessus, Metasploit, Snort, Suricata, Wireshark, Hashcat, John the Ripper Guías de configuración básica de firewalls y routers Modelos de informes técnicos de vulnerabilidades Plantillas de inventario de activos y matrices de criticidad Listados de usuarios, accesos y permisos simulados Informes de amenazas regionales (por ejemplo, ESET, Fortinet, Kaspersky) Política de uso aceptable

	Política de control de accesos Política de respaldo y recuperación Política de manejo de incidentes de seguridad

UNIDAD DE COMPETENCIA (UC)	
UC 5: Gestionar los riesgos asociados a los activos informáticos y procesos críticos de una organización, proponiendo acciones preventivas y de recuperación, conforme a principios básicos de gestión del riesgo, continuidad operativa y recuperación de la información, para minimizar el incidentes y mantener la disponibilidad de los sistemas.	
Elementos de competencia (EC)	**Criterios de desempeño (CD)**
EC1: Analizar riesgos asociados a activos informáticos y procesos críticos, aplicando métodos básicos de análisis de riesgos y relacionando vulnerabilidades con posibles incidentes.	CD1.1: Clasifica los activos informáticos esenciales en la operación de servicios educativos, institucionales o comunitarios.
	CD1.2: Cataloga amenazas comunes que pueden afectar la disponibilidad, integridad o confidencialidad de los sistemas.
	CD1.3: Emplea métodos básicos como matrices de riesgo o formatos simplificados basados en NIST SP 800-30 o ISO/IEC 27005 para clasificar riesgos.
	CD1.4: Relaciona vulnerabilidades existentes con posibles incidentes que generen impacto en los servicios.
	CD2.1: Diferencia entre continuidad operativa y recuperación ante desastres en el contexto de la seguridad de la información.
	CD2.2: Selecciona componentes clave de un plan básico: BIA, RTO, RPO, responsables, procedimientos y pruebas.
	CD2.3: Interpreta los simulacros de recuperación ante incidentes críticos.

EC2: Aplicar conceptos básicos de continuidad operativa y recuperación ante desastres, realizando simulacros referentes a interrupciones del servicio.	CD2.4: Documenta procedimientos sencillos de respaldo, restauración y roles ante interrupciones del servicio.
EC3: Evaluar los riesgos en función de su impacto y probabilidad, empleando herramientas y plantillas estandarizadas según prioridades.	CD 3.1: Diferencia riesgos tolerables y no tolerables conforme al contexto y recursos disponibles.
	CD3.2: Calcula niveles de riesgo combinando impacto y probabilidad en un entorno simulado o escolar.
	CD3.3: Organiza el análisis mediante plantillas, hojas de cálculo o herramientas digitales accesibles.
	CD3.4: Presenta los resultados del análisis de forma clara, argumentando prioridades y recomendaciones.
EC4: Proponer medidas básicas de tratamiento del riesgo informático priorizando su implementación según el contexto organizacional, la criticidad de los activos y la viabilidad de los recursos disponibles.	CD4.1: Propone controles preventivos, detectivos o correctivos reduciendo la exposición al riesgo.
	CD4.2: Relaciona las propuestas con buenas prácticas o lineamientos normativos básicos de seguridad digital.
	CD4.3: Prioriza medidas realistas basadas en el nivel de riesgo residual, recursos disponibles y criticidad.
	CD4.4: Justifica la viabilidad técnica y económica de las medidas sugeridas en el contexto de una organización real o simulada.
Espacios e instalaciones:	Entorno de aprendizaje Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización. Acceso a laboratorio virtual (local o en la nube) para simulaciones controladas.

Insumos y recursos:	**Sistemas Operativos (mínimos requeridos y recomendados):** • Windows 10 u 11 (mínimo requerido) • Ubuntu Desktop (mínimo requerido) • Kali Linux (mínimo requerido) • Parrot OS (recomendado para prácticas ofensivas) • Rocky Linux o CentOS Stream (recomendado para administración de servidores) **Virtualización y entornos controlados:** • VirtualBox (mínimo requerido) • VMware Workstation o Player (mínimo requerido) • Hyper-V (recomendado) • VMware ESXi (recomendado para prácticas avanzadas o institucionales) **Conectividad:** • Internet de alta velocidad (mínimo requerido) • Red interna aislada para simulacros y ejercicios de ciberseguridad • Herramientas de Seguridad y Análisis **Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad)

	• Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Laboratorios virtuales y simuladores:** • Máquinas virtuales locales (VirtualBox o VMware) • TryHackMe (recomendado) • VulnHub (recomendado) • OWASP Juice Shop (recomendado para prácticas de seguridad web) • Cyber Range local o institucional (recomendado) **Plataformas Educativas y de Apoyo Didáctico:** • Moodle o Google Classroom (mínimo requerido) • draw.io o similares para diagramación técnica (recomendado) • LibreOffice o software ofimático compatible (mínimo requerido) • Trello o herramienta tipo Kanban (recomendado para gestión de tareas) • Herramientas de Monitoreo y Gestión de Incidentes **Monitoreo de redes y sistemas:** • Nagios (recomendado) • Zabbix (recomendado) • Grafana (recomendado) **Gestión de tickets e incidentes:** • GLPI o OTRS (recomendado) **Sistemas de detección y análisis:** • Consolas básicas de Snort (mínimo requerido)

	• Suricata integrado con Kibana o ELK Stack (recomendado) **Hardware complementario:** • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado) • Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)
Información utilizada:	Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible) NIST SP 800-30 (análisis de riesgos) NIST SP 800-53 (controles de seguridad para sistemas de información) ISO/IEC 27001 (gestión de la seguridad de la información) ISO/IEC 27002 (controles de seguridad) OWASP Top 10 (riesgos en aplicaciones web) MITRE ATT&CK (catálogo de técnicas y tácticas de ataque) Ley Orgánica de Protección de Datos Personales (LOPDP) Código Orgánico Integral Penal (COIP), sección delitos informáticos Ley de Comercio Electrónico, Firmas y Mensajes de Datos Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles) CIS Benchmarks para hardening de sistemas Guías de configuración segura de NIST Manuales institucionales o académicos para Windows/Linux Manuales y documentación de herramientas como Nmap, Nessus, Metasploit, Snort, Suricata, Wireshark, Hashcat, John the Ripper Guías de configuración básica de firewalls y routers Modelos de informes técnicos de vulnerabilidades Plantillas de inventario de activos y matrices de criticidad

	Listados de usuarios, accesos y permisos simulados Informes de amenazas regionales (por ejemplo, ESET, Fortinet, Kaspersky) Política de uso aceptable Política de control de accesos Política de respaldo y recuperación Política de manejo de incidentes de seguridad

UNIDAD DE COMPETENCIA (UC)	
UC 6: Promover la cultura de seguridad informática en el entorno escolar, empresarial o comunitario, aplicando prácticas seguras y prevención de incidentes, contribuyendo a la creación de entornos digitales confiables.	
Elementos de competencia (EC)	**Criterios de desempeño (CD)**
EC1: Aplicar buenas prácticas de seguridad informática en distintos contextos incorporando medidas de protección y procedimientos de prevención de incidentes.	CD1.1: Muestra buenas prácticas de protección de datos personales y corporativos en actividades escolares, laborales y comunitarias.
	CD1.2: Reporta comportamientos o incidentes que comprometen la seguridad de la información, conforme a protocolos básicos.
	CD1.3: Utiliza contraseñas robustas, cifrado y respaldos como mecanismos esenciales de protección.
	CD1.4: Emplea principios como consentimiento informado y privacidad en el tratamiento de datos personales.
EC2: Fomentar comportamientos seguros mediante recursos digitales y acciones formativas adaptando los mensajes y materiales al contexto y necesidades del entorno.	CD2.1: Distingue necesidades y riesgos del entorno para diseñar estrategias de sensibilización contextualizadas.
	CD2.2: Selecciona contenidos relevantes sobre amenazas, buenas prácticas y normas de ciberseguridad básicas.
	CD2.3: Formula mensajes claros sobre el uso responsable de la tecnología, protección de datos y manejo ético de contraseñas.

	CD2.4: Elabora materiales visuales o digitales para difundir mensajes de cultura de seguridad en su entorno.
EC3: Diseñar estrategias de sensibilización en ciberseguridad adaptadas al entorno, integrando recursos apropiados para el público objetivo.	CD3.1: Distingue las necesidades, características y riesgos específicos del entorno en la construcción de estrategias de sensibilización.
	CD3.2: Selecciona contenidos relevantes sobre amenazas, buenas prácticas y normas de seguridad digital, adecuadas al público objetivo.
	CD3.3: Crea mensajes claves sobre el uso responsable de las tecnologías, protección de datos personales y gestión segura de contraseñas.
	CD3.4: Elabora materiales de apoyo de sensibilización en ciberseguridad para difundir en su entorno social, educativo u organizacional.
EC4: Promover el uso ético, legal y responsable de los recursos informáticos en diferentes contextos, integrando estrategias que fomenten la protección de la información y la propiedad intelectual.	CD4.1: Selecciona normativas básicas sobre el uso adecuado de tecnología y protección de la propiedad intelectual.
	CD4.2: Distingue las practicas inadecuadas o riesgosas en el uso de la información y propone alternativas responsables.
	CD4.3: Aplica el uso responsable y consciente de tecnologías digitales en contextos educativos, sociales o laborales.
	CD4.4: Propone estrategias que fomenten el respeto por los derechos de autor, licencias de software y uso correcto de contenidos digitales.
Condiciones de ejecución de la Unidad de Competencia:	
Espacios e instalaciones:	Entorno de aprendizaje Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización.

	Acceso a laboratorio virtual (local o en la nube) para simulaciones controladas.
Insumos y recursos:	**Sistemas Operativos (mínimos requeridos y recomendados):** • Windows versión actualizada (mínimo requerido) • Linux versión actualizada (mínimo requerido) • Kali Linux (mínimo requerido) • Parrot OS (recomendado para prácticas ofensivas) • Rocky Linux o CentOS Stream (recomendado para administración de servidores) **Virtualización y entornos controlados:** • VirtualBox (mínimo requerido) • VMware Workstation o Player (mínimo requerido) • Hyper-V (recomendado) • VMware ESXi (recomendado para prácticas avanzadas o institucionales) • Entornos en la nube **Conectividad:** • Internet de alta velocidad (mínimo requerido) • Red interna aislada para simulacros y ejercicios de ciberseguridad • Herramientas de Seguridad y Análisis **Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework

	• Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Laboratorios virtuales y simuladores:** • Máquinas virtuales locales (VirtualBox o VMware) • TryHackMe (recomendado) • VulnHub (recomendado) • OWASP Juice Shop (recomendado para prácticas de seguridad web) • Cyber Range local o institucional (recomendado) **Plataformas Educativas y de Apoyo Didáctico** • Moodle o Google Classroom (mínimo requerido) • draw.io o similares para diagramación técnica (recomendado) • LibreOffice o software ofimático compatible (mínimo requerido) • Trello o herramienta tipo Kanban (recomendado para gestión de tareas) • Herramientas de Monitoreo y Gestión de Incidentes **Monitoreo de redes y sistemas:** • Nagios (recomendado) • Zabbix (recomendado) • Grafana (recomendado)

	Gestión de tickets e incidentes: • GLPI o OTRS (recomendado) **Sistemas de detección y análisis:** • Consolas básicas de Snort (mínimo requerido) • Suricata integrado con Kibana o ELK Stack (recomendado) **Hardware complementario:** • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado) • Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)
Información utilizada:	Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible) NIST SP 800-30 (análisis de riesgos) NIST SP 800-53 (controles de seguridad para sistemas de información) ISO/IEC 27001 (gestión de la seguridad de la información) ISO/IEC 27002 (controles de seguridad) OWASP Top 10 (riesgos en aplicaciones web) MITRE ATT&CK (catálogo de técnicas y tácticas de ataque) Ley Orgánica de Protección de Datos Personales (LOPDP) Código Orgánico Integral Penal (COIP), sección delitos informáticos Ley de Comercio Electrónico, Firmas y Mensajes de Datos Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles) CIS Benchmarks para hardening de sistemas Guías de configuración segura de NIST Manuales institucionales o académicos para Windows/Linux

	Manuales y documentación de herramientas como Nmap, Nessus, Metasploit, Snort, Suricata, Wireshark, Hashcat, John the Ripper Guías de configuración básica de firewalls y routers Modelos de informes técnicos de vulnerabilidades Plantillas de inventario de activos y matrices de criticidad Listados de usuarios, accesos y permisos simulados Informes de amenazas regionales (por ejemplo, ESET, Fortinet, Kaspersky) Política de uso aceptable Política de control de accesos Política de respaldo y recuperación Política de manejo de incidentes de seguridad

UNIDAD DE COMPETENCIA (UC)	
UC 7: Realizar auditorías básicas de seguridad informática, generando informes técnicos, basados en la normativa legal para evaluar el cumplimiento, detección de vulnerabilidades y proponer acciones correctivas.	
Elementos de competencia (EC)	**Criterios de desempeño (CD)**
EC1: Aplicar herramientas y técnicas de recolección de información que permitan la evaluación del estado de seguridad de sistemas y redes.	CD1.1: Selecciona herramientas de recolección de información adecuadas según el tipo de sistema, red o infraestructura evaluada.
	CD1.2: Distingue configuraciones inseguras, servicios expuestos y otros factores de riesgo utilizando criterios técnicos básicos.
	CD1.3: Aplica procedimiento de escaneo y análisis sin afectar la disponibilidad ni la integridad de los sistemas evaluados.

	CD1.4: Emplea principios éticos y legales durante el análisis de la información recolectada, evitando acciones intrusivas o no autorizadas.
EC2: Planear auditorías básicas de seguridad informática en función de los objetivos y alcances definidos, integrando recursos y actores involucrados.	CD2.1: Selecciona los activos informáticos que serán objeto de evaluación, considerando su importancia en la operación organizacional.
	CD2.2: Establece una metodología básica de auditoría, con fases, actividades y herramientas, basada en la normativa vigente
	CD2.3: Elabora un cronograma con tiempos estimados para cada fase del proceso de auditoría.
	CD2.4: Diseña un plan de auditoría claro, estructurado y comprensible para todos los actores involucrados.
EC3: Elaborar informes técnicos que incluyan hallazgos, evidencias, conclusiones y recomendaciones, presentados de manera estructurada y comprensible.	CD3.1: Describe los hallazgos de seguridad de manera precisa, basada en los datos recolectados durante la auditoría.
	CD3.2: Analiza los riesgos asociados a las vulnerabilidades encontradas, considerando impacto y probabilidad.
	CD3.3: Formula conclusiones coherentes con los hallazgos y alineadas con los objetivos del plan de auditoría.
	CD3.4: Propone recomendaciones específicas y viables, basadas en buenas prácticas de seguridad.
EC4: Organizar la presentación de resultados de la auditoría a los actores involucrados de manera ética y profesional.	CD4.1: Selecciona medios y recursos apropiados para presentar los resultados de manera clara y efectiva.
	CD4.2: Elabora las presentaciones adaptadas al perfil técnico o directivo de los destinatarios.
	CD4.3: Expone las recomendaciones fomentando la mejora continua y la adopción de buenas prácticas.

	CD4.4: Integra la retroalimentación recibida para fortalecer futuras auditorías y procesos de mejora.
	CD4.5: Presenta el informe final de la auditoria con base a los hallazgos encontrados
Condiciones de ejecución de la Unidad de Competencia:	
Espacios e instalaciones:	Entorno de aprendizaje Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización. Acceso a laboratorio virtual (local o en la nube) para simulaciones controladas.
Insumos y recursos:	**Sistemas Operativos (mínimos requeridos y recomendados):** • Windows 10 u 11 (mínimo requerido) • Ubuntu Desktop (mínimo requerido) • Kali Linux (mínimo requerido) • Parrot OS (recomendado para prácticas ofensivas) • Rocky Linux o CentOS Stream (recomendado para administración de servidores) **Virtualización y entornos controlados:** • VirtualBox (mínimo requerido) • VMware Workstation o Player (mínimo requerido) • Hyper-V (recomendado) • VMware ESXi (recomendado para prácticas avanzadas o institucionales) • En la nube

	Conectividad: • Internet de alta velocidad (mínimo requerido) • Red interna aislada para simulacros y ejercicios de ciberseguridad • Herramientas de Seguridad y Análisis **Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Laboratorios virtuales y simuladores:** • Máquinas virtuales locales o en la nube (VirtualBox o VMware) • TryHackMe (recomendado) • VulnHub (recomendado) • OWASP Juice Shop (recomendado para prácticas de seguridad web) • Cyber Range local o institucional (recomendado) **Plataformas Educativas y de Apoyo Didáctico:** • Moodle o Google Classroom (mínimo requerido)

	• draw.io o similares para diagramación técnica (recomendado) • LibreOffice o software ofimático compatible (mínimo requerido) • Trello o herramienta tipo Kanban (recomendado para gestión de tareas) • Herramientas de Monitoreo y Gestión de Incidentes **Monitoreo de redes y sistemas:** • Nagios (recomendado) • Zabbix (recomendado) • Grafana (recomendado) **Gestión de tickets e incidentes:** • GLPI o OTRS (recomendado) **Sistemas de detección y análisis:** • Consolas básicas de Snort (mínimo requerido) • Suricata integrado con Kibana o ELK Stack (recomendado) **Hardware complementario:** • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado) • Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)
Información utilizada:	Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible) NIST SP 800-30 (análisis de riesgos)

	NIST SP 800-53 (controles de seguridad para sistemas de información) ISO/IEC 27001 (gestión de la seguridad de la información) ISO/IEC 27002 (controles de seguridad) OWASP Top 10 (riesgos en aplicaciones web) MITRE ATT&CK (catálogo de técnicas y tácticas de ataque) Ley Orgánica de Protección de Datos Personales (LOPDP) Código Orgánico Integral Penal (COIP), sección delitos informáticos Ley de Comercio Electrónico, Firmas y Mensajes de Datos Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles) CIS Benchmarks para hardening de sistemas Guías de configuración segura de NIST Manuales institucionales o académicos para Windows/Linux Manuales y documentación de herramientas como Nmap, Nessus, Metasploit, Snort, Suricata, Wireshark, Hashcat, John the Ripper Guías de configuración básica de firewalls y routers Modelos de informes técnicos de vulnerabilidades Plantillas de inventario de activos y matrices de criticidad Listados de usuarios, accesos y permisos simulados Informes de amenazas regionales (por ejemplo, ESET, Fortinet, Kaspersky) Política de uso aceptable Política de control de accesos Política de respaldo y recuperación Política de manejo de incidentes de seguridad

UNIDAD DE COMPETENCIA (UC)	
UC8: Aplicar fundamentos del hacking ético y análisis forense básico en la evaluación de la seguridad de sistemas y redes en entornos controlados, interpretando hallazgos, proponiendo mejoras de protección y cumpliendo principios legales y éticos.	
Elementos de la competencia (EC)	**Criterios de desempeño (CD)**
EC1: Diferenciar el hacking ético del hacking malicioso, destacando el rol del consentimiento y aplicando normativa vigente.	CD1.1: Analiza los principios del hacking ético, incluyendo legalidad, autorización, confidencialidad y responsabilidad profesional.
	CD1.2: Distingue las fases de una prueba de penetración (reconocimiento, escaneo, explotación simulada y reporte).
	CD1.3: Aplica técnicas básicas de reconocimiento y escaneo de vulnerabilidades utilizando herramientas autorizadas y en entornos simulados.
	CD1.4: Documenta los hallazgos de forma técnica, sin comprometer la operación o integridad del entorno evaluado.
EC2: Emplear herramientas básicas de análisis forense para recolectar y preservar evidencia digital, asegurando la integridad, trazabilidad de los hallazgos en entornos controlados.	CD 2.1: Distingue conceptos clave del análisis forense: cadena de custodia, integridad de la evidencia, duplicación forense.
	CD2.2: Utiliza herramientas básicas de adquisición y análisis de datos digitales en discos o sistemas de archivos.
	CD2.3: Aplica procedimientos de preservación de evidencia en entornos simulados, asegurando su integridad y trazabilidad.
	CD2.4: Describe hallazgos relevantes derivados del análisis forense, considerando su valor probatorio en contextos educativos o institucionales.
EC3: Interpretar los hallazgos de pruebas éticas y análisis forense básico para apoyar decisiones de seguridad, evaluando el origen	CD3.1: Relaciona las vulnerabilidades encontradas con los riesgos de seguridad identificados.
	CD3.2: Evalúa la información obtenida en análisis forense para comprender el origen y tipo de incidente simulado.
	CD3.3: Propone medidas preventivas o correctivas básicas basadas en los hallazgos.

de incidentes y presentando resultados de forma clara y estructurada.	CD3.4: Presenta los resultados de manera clara, estructurada y respetando principios de confidencialidad.
EC4: Aplicar principios legales y éticos en todas las etapas del hacking ético y análisis forense básico, respetando normativa legal, marcos éticos y consentimiento.	CD4.1: Distingue los límites legales del hacking ético en Ecuador, incluyendo delitos informáticos definidos en el COIP.
	CD4.2: Reconoce los marcos éticos y normativos internacionales que rigen el análisis forense y las pruebas de penetración (ej. EC-Council, NIST).
	CD4.3: Justifica la importancia del consentimiento informado y la autorización previa en toda práctica de evaluación de seguridad.

5. Relación de las Unidades de competencia de la Figura profesional Seguridad Informática y módulos de especialización

Tabla 1. Relación Unidades de competencia – módulo de especialización

No.	Unidad de Competencia	Módulo de especialización
1	Analizar el estado de seguridad y vulnerabilidades de la red y de los sistemas informáticos, con el fin de reducir amenazas y proponer soluciones digitales.	Fundamentos de Seguridad Informática
2	Aplicar protocolos de respuesta ante incidentes, recuperando sistemas y respaldos de información, garantizando la continuidad operativa de los servicios.	Manejo de incidentes y recuperación informática
3	Realizar el monitoreo de redes y sistemas informáticos en forma periódica en la detección de eventos de seguridad y riesgos, aplicando herramientas de supervisión, análisis de datos y elaboración de reportes técnicos conforme a protocolos establecidos, con el fin de mantener la disponibilidad y confiabilidad de los servicios.	Monitoreo de redes y sistemas informáticos
5	Gestionar los riesgos asociados a los activos informáticos y procesos críticos de una organización, proponiendo acciones preventivas y de recuperación, conforme a principios básicos de gestión del riesgo, continuidad operativa y recuperación de la información, para minimizar incidentes y mantener la disponibilidad de los sistemas.	Gestión y análisis de Vulnerabilidades
7	Realizar auditorías básicas de seguridad informática, generando informes técnicos, basados en la normativa legal para evaluar el cumplimiento, detección de vulnerabilidades y proponer acciones correctivas.	Auditorías básicas de seguridad informática
4	Emplear normas de protección de datos y de ciberseguridad en sistemas informáticos, garantizando la protección de información sensible.	Cultura y Conciencia en Ciberseguridad
6	Promover la cultura de seguridad informática en el entorno escolar, empresarial o comunitario, aplicando prácticas seguras, prevención de incidentes, contribuyendo a la creación de entornos digitales confiables.	

8	Aplicar fundamentos del hacking ético y análisis forense básico en la evaluación de la seguridad de sistemas y redes en entornos controlados, interpretando hallazgos, proponiendo mejoras de protección y el cumpliendo principios legales y éticos.	