Tabla del número de ítems por resultados de aprendizaje del programa de estudio Prueba Nacional Escrita Comprensiva de Especialidades en Educación Técnica 2024
Convocatoria ordinaria y extraordinaria (aplazados)
CIBERSEGURIDAD 2024

Estimado docente:

A continuación, se le suministra el número de ítems que tendrá la Prueba Nacional Escrita Comprensiva Estandarizada dela especialidad, según la distribución de objetivos adaptados y contenidos del programa de estudio para el periodo lectivo 2024, de acuerdo con la consulta realizada a los docentes en las diferentes regiones educativas del país.

Tema	Resultado de Aprendizaje	Indicador de logro	Contenidos	N° ítems
HERRAMIENTAS PARA LA PRODUCCIÓN DE DOCUMENTOS	1. Diferenciar las funciones y herramientas disponibles en la creación de documentos, hojas electrónicas tanto en ambiente local, su aplicación en entornos web y su importancia en la comunicación.	• Identifica las funciones disponibles para la creación, apertura, edición e impresión de documentos. • Identifica las operaciones básicas que se ejecutan	Editor de Texto • Generalidades • Trabajo con documentos • Formato de documentos • Manejo de bloques • Tablas y gráficos en un documento Hoja Electrónica • Características de la hoja electrónica • Creación de una hoja de cálculo • Recuperación y edición • Utilización de fórmulas	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

		en la hoja de cálculo. • Identifica las herramientas que proporciona el entorno web para la comunicación, mensajería instantánea y visualización de imágenes.	• Formatos • Creación de gráficos • Tablas dinámicas Herramientas para la web • Formularios en línea • Almacenamiento Entorno Web • Correo electrónico • Redes sociales • Videoconferencia. • Realidad aumentada. • Inteligencia artificial • Simuladores • Industria 4.0	

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
HERRAMIENTAS PARA LA GESTIÓN Y ANÁLISIS DE LA INFORMACIÓN	2. Distinguir los elementos de las bases de datos y su contexto en el reconocimiento de los principios éticos y legales.	• Identifica los tipos de datos y su relación con bases de datos. • Distingue los elementos de la base de datos.	Datos Base de datos • Elementos de las Bases de Datos Entorno Trabajo con Operaciones básicas • Consultas Aprendizaje automatizado delos datos Arquitectura para datos masivos Ingeniería de Datos Ética • Legislación vigente relacionada con el tratamiento de los datos	**2**
INTERNET DE TODO Y SEGURIDAD DE LOS DATOS.	3. Evaluar las características del ámbito de la ciberseguridad, sus principios y las medidas de	• Identifica las formas de transmisión de las tecnologías.	Transición a IdT • Las conexiones de IdT • Tecnología de la información (TI) • Tecnología Operativa (TO) en IdT	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

	seguridad cibernética del Internet del todo y su importancia para la protecciónе integridad de los datos mediante el uso de tecnologías.		• Conexiones Máquina a Máquina (M2M) • Conexiones Máquina a Persona (M2P) • Conexiones de redes entre pares (P2P) • Implementación de una solución de IdT • Seguridad e IdT Unificación de todo • Creación de modelos de una solución IdT • Interacciones de IdT en un modelo • Creación de un prototipo para sus ideas • Recursos para la creación de prototipos • Oportunidades de aprendizaje. • Ejemplos de IdT	
ESQUEMAS LÓGICOS PARA EL DISEÑO SEGURO DEL SOFTWARE	4. Reconocer técnicas de programación y los tipos de condicionales,	• Reconoce técnicas de programación requeridas en los procesos lógicos de	Conceptos Básicos • Técnicas de programación • Características de los algoritmos	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

	ciclos de repetición en las que se implementen variables y operadores mediante métodos de conocimiento lógicos algorítmicos.	resolución de problemas cotidianos. • Identifica ciclos condicionales y de repetición.	• Variables • Tipos de datos • Operadores Condicionales Bucles Otros • Funciones • Clases • Objetos	

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
PROGRAMACIÓN INTERPRETADA MULTIPARADIGMA	5. Identificar los elementos del entorno de desarrollo con programación interpretada multiparadigma.	• Reconoce los elementos que conforman el entorno IDE para el trabajo de programación interpretada multiparadigma.	Introducción a la programación interpretada multiparadigma • Concepto • Modo intérprete y su entorno • Código fuente • Números • Cadenas de caracteres Listas	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

PROGRAMACIÓN INTERPRETADA MULTIPARADIGMA	6. Describir las sintaxis para la elaboración de programa aplicando las herramientas de control de flujo, estructuras de datos y módulos.	• Identifica la codificación de programas que utilicen herramientas de control.	Herramientas de control de flujo • Sentencia if • Sentencia for • Función Range () • Sentencias: Break, continue y else • Sentencia pass • Argumentos con valores por omisión • Palabras claves como argumentos • Listas de argumentos • Desempaquetado Estructuras de datos • Pilas • Colas • Listas anidadas • Tuplas y secuencias • Técnicas de iteración Módulos • Módulos scripts • Función dir ( ) • Paquetes ○ Importaciones	**3**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

PROGRAMACIÓN INTERPRETADA MULTIPARADIGMA	7. Programar aplicaciones web utilizando los elementos del entorno de desarrollo utilizando programación interpretada multiparadigma.	• Identifica manejo de errores, excepciones, clases, herencia entre otros.	Flujo de entrada y salida de datos • Entrada de datos • Formateo de cadenas • Escritura de archivos • Métodos de objetos de archivo • Guardar datos estructurados Errores y excepciones • Errores y sintaxis • Excepciones • Levantado de excepciones • Excepciones definidas por el usuario Clases • Nombres y objetos • Ámbito y espacios de nombres • Objetos de clase Objetos instancia	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
APLICACIONES DE LA ROBÓTICA	8. Discriminar los principios y usos de la automatización robotizada empleada en procesos de producción y bienestar social.	• Reconoce conceptos básicos de la automatización robotizada.	Automatización robotizada • Concepto • Características • Campo de acción • Percepción y razonamiento • Procesos y tecnologías Usos • Industria • Áreas de bienestar social • Empresa • Hogar • Educación	**1**

APLICACIONES DE LA ROBÓTICA	9. Analizar el uso de los motores y simuladores por medio de retos específicos.	• Identifica conceptos relacionados con control, motores y simuladores.	Control
			• Mecánico y eléctrico
			• Tipos de circuitos
			• Serie
			• Paralelo
			• Combinados
			• Motores
			  • Tipos de motores
			  • Usos
			Simuladores
				2

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
			• Simuladores eléctricos • Simuladores informáticos	
FUNDAMENTOS DE CIBERSEGURIDAD	10. Reconoce los conceptos básicos relacionados conla gestión de contraseñas y defensa activas.	• Reconoce los conceptos básicos relacionados con la gestión de contraseñas y defensa activa.	Control de acceso y gestiónde contraseñas • Conceptos • Ransomware • Malware • Hacktivistas • Firmware o soporte lógico inaltarable • Sombrero negro Papel de las contraseñas Defensa activa • Herramientas OpenSSL • Métodos • Técnicas • IDS (Sistemas de Detección de Intrusos) • IPS (Sistemas de Prevención de Intrusos)	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
			Planes de contingencia	
FUNDAMENTOS DE CIBERSEGURIDAD	11. Reconoce los elementos generadores del proceso de aplicación de criptografía	• Reconoce los elementos generadores del proceso de aplicaciónde criptografía.	Criptografía • Concepto • Tipos de cifrado • Esteganografía • Algoritmos • Aplicaciones • Defensa en profundidad Estrategias para implementar una seguridadefectiva	**1**
FUNDAMENTOS DE TECNOLOGÍAS DE INFORMACIÓN	12. Emplear los componentes requeridos para la construcción, reparación o actualización de computadoras personales aplicando principios de salud ocupacional.	• Identifica los componentes que se requieren en las labores de ensamble, actualización y reparación de computadores personales.	Computadoras personales • Funcionamiento • Componentes • Características • Funciones • Componentes Desmontaje de la computadora Ensamble de la computadora	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
OPORTUNIDADES DE NEGOCIOS	13. Identificar habilidades y responsabilidades de la persona emprendedora.	• Identifica habilidadesy responsabilidades de la persona emprendedora. • Identifica las oportunidades del mercado según las nuevas tendencias.	Emprendimiento: • Definición, características e importancia del fomento del espíritu emprendedor. • Características de la cultura emprendedora. • Uso productivo de las tecnologías en los negocios. Mercado: • Concepto. • Funcionamiento del mercado y tendencias innovadoras. • Detección del mercado y clientes potenciales. • El cliente como elemento clave.	**1**
OPORTUNIDADES DE NEGOCIOS	14. Proponer soluciones creativas e innovadoras a necesidades y	• Identifica la importancia de la creatividad e innovación en los aspectos cotidianos de su quehacer.	Creatividad e Innovación • Concepto • Importancia • El proceso de la creatividad y la habilidad de pensar	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
	oportunidades del mercado.		creativamente • Innovación y su proceso • Tipos de innovación y cómo diferenciarlos	
MODELO DE NEGOCIOS	15. Distinguir las características de los aspectos que deben considerarse parala implementacióndel plan de puesta en marchadel modelo de negocio.	• Distingue los aspectos que se consideran en la construcción de un modelo de negocio. • Identifica los aspectos que deben considerarse en la puesta en marcha delmodelo de negocios.	Modelo de negocios: • Concepto. • Aspectos a considerar: ○ Clientes. ○ Canales. ○ Relación con los clientes. Plan de implementación: • Inversión inicial. • Diseño de marca. • Plan de mercadeo y ventas: ○ Impacto social. ○ Ambiental. Estrategias para la negociación.	**1**
CREACIÓN DE LA EMPRESA	16. Identificar los elementos que conforman el plan de negocios.	• Selecciona el tipo de empresa para el desarrollo de su modelo de negocio. • Identifica los elementos que	Tipos de empresa: • Concepto. • Características. • Ventajas. • Desventajas. Plan de negocios:	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
		conforman el plan de negocios.	• Modelo de negocios. • Estudios de mercado. Estructuración del negocio, según el modelo empresarial: • Estructuración del negocio, según el modelo empresarial. • Unidades y departamentos de la empresa.	
SISTEMAS OPERATIVOS	17. Distinguir procesos avanzados de configuración de sistemas operativos.	• Identifica el concepto de compatibilidad de los sistemas operativos. • Reconoce los conceptos multiarranque, directorio, archivo, GUI, herramientas administrativas y herramientas de sistema.	Actualizaciones del sistema operativo. Instalación de sistemas operativos. Procesos avanzados de configuración: • Multiarranque. • Estructuras de directorios y atributos de archivos. • GUI y el panel de control. • Versiones. • Técnicas de mantenimiento preventivo. Procesos de diagnóstico de	**3**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
			fallas.	
CICLOS DE DESARROLLO SEGURO	18. Aplicar las etapas para la supervivencia de sistemas en la elaboración de software seguro.	• Reconoce el concepto de riergo de seguridad. • Identifica las valoraciones y riesgos del ciclo de vida de sistemas. • Reconoce las capas de protección de software.	Gestión del riesgo de seguridad: • Valoración del riesgo de sistemas. • Amenazas en los sistemas de software. Diseño para la seguridad. Supervivencia de sistemasde software: • Concepto. • Etapas en el análisis de supervivencia de sistemas.	**3**
SEGURIDAD EN LA NUBE	19. Distinguir características de los servicios en la nube según el modelo relación yel tipo de servicio nube.	• Reconoce conceptos relacionados con computación en la nube y modelos de negocio. • Identifica conceptos y formas de organización nube IaaS, PaaS y SaaS. • Identifica aplicaciones en forma segura en entornos de computación en la nube.	Computación en la nube: • Cloud computing. • Máquina virtual. Virtualización: • Concepto. • Tipos de virtualización. • Rol de la virtualización. • Software de virtualización. Computación en la nube: • Características. • Tipos de soluciones.	**3**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
			• Ventajas. • Desventajas. • Seguridad. Componentes computacionales en la nube: • Nube pública. • Nube privada. • Nube híbrida. Seguridad de datos en la nube: • Rendimiento. • Automatización. • Control de consumo. • Control de rendimiento. • Cloud first. Aplicación de seguridad enla nube: • Concepto cloudbroker. • Amenazas y riesgos. Administración de seguridaden la nube.	
ÉTICA EN LA CIBERSEGURIDAD	20. Distingue habilidades requeridas en las personas que	• Identifica conceptos, tipos, ventajas y desventajas del hackeo ético.	Generalidades de hackeo ético: • Hackeo. • Hackeo ético. • Adware.	**4**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
	realicen hackeo ético.		• Ataque. • Puerta trasera. • Bot. • Phishing. • Bomba lógica. • Malware. • Suplantación de identidad. • Spyware. • Ciberdelincuentes. Tipos de hacker: • Sombrero blanco. • Sombrero gris. • Sombrero negro. Habilidades de hackeo ético: • Computación. • Redes. • Linux. • Virtualización. • Seguridad TI. • Tecnología inalámbrica. Fases de hackeo ético. Desarrollo de planes de hackeo ético.	
EFICIENCIA ENERGÉTICA	21. Identificar conceptos y principios	• Identifica conceptos y principios eléctricos relacionados con la	Principios eléctricos. Eficiencia energética: • Concepto de	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
	eléctricos relacionados conla eficiencia energética.	eficiencia energética.	eficiencia energética. • Generalidades de la eficiencia energética. • Eficiencia energética en el sector de las tecnologías de la información. Orientaciones generales y consumo eléctrico: • Eficiencia eléctrica enel hogar y empresarial. • Estimaciones de consumo eléctrico. • Interpretación de etiquetas eléctricas. Tecnologías y soluciones para una optimización energética de los sistemasTI: • Equipos de Hardware. • Software y gobernanza TI. Gestión energética eficienteen los Sistemas de Información.	
EFICIENCIA ENERGÉTICA	22. Comparar disposiciones	• Señala disposiciones nacionales	Plan nacional de energía • Políticas	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítem
	nacionales e internacionales que sean amigables con el ambiente para el desarrollo sostenible energético.	relacionadas con políticas leyes y reglamentos orientados al desarrollo energético sostenible.	• Leyes • Reglamentos de desarrollo energético sostenible	
FUNDAMENTOS DE ENRUTAMIENTO Y CONMUTACIÓN.	23. Identificar la configuración básica de dispositivos de red con simuladores y equipo físico, relacionados con redes de área local e inalámbricas.	• Reconoce las características de DHCPv4. • Distingue las características de DHCPv6. • Identifica conceptos relacionados con redes de área local inalámbricas.	Configuración básica de dispositivos de red. Conceptos de conmutación. Conceptos de VLAN. DHCPv4. DHCPv6. Conceptos de seguridad LAN. LAN inalámbricas. • Conceptos • Introducción y componentes Enrutamiento.	**3**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
INFORMÁTICA FORENSE Y SOFTWARE MALICIOSO.	24. Reconocer conceptos, características, causas, procedimientosy principios aplicados en la informática forense.	• Reconoce conceptos, características, causas, procedimientos y principios aplicados en lainformática forense. • Identifica herramientas requeridas en peritajes forenses. • Identifica conceptos y la clasificación de software maliciosos.	Informática forense: • Ciencia forense. • Informática forense. • Software malicioso. Métodos de seguridad: • Patrón de bloqueo. • Pin de bloqueo. • Contraseña. • Huella dactilar. • Desbloqueo facial. • Cifrado de información. Software malicioso o malware: • Virus. • Gusano. • Troyano. • Adware. • Keylogger. • Crimeware.	**3**
DERECHO INFORMÁTICO Y GOBERNANZA DE DATOS.	25. Interpretar normativas jurídicas nacionales e internacionales con respecto al	• Identifica los aspectos requeridos en el programa de gobernanza de datos.	Marco jurídico de protección de datos mundial y nacional	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
	derecho informático y gobernanza de datos.		Sistemas de gestión (buenas prácticas): • Leyes • Decretos • NIST • ISO 20000 • ISO 27001	
DEFENSA DE APLICACIONES WEB Y MÓVILES.	26. Reconocer las tendencias del diseño seguro en el desarrollo de diferentes tipos de aplicaciones web y móviles.	• Identifica los tipos de factores de riesgo en las aplicaciones móviles.	Generalidades en la seguridadde las aplicaciones: • Conceptos. • Evolución de las aplicaciones. • Funcionalidades. Autentificación de usuarios. Tipos de amenazas. Prevención ante ataques directosal usuario. Factores de riesgo en las aplicaciones móviles: • Concepto. • Riesgos de red.	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
			• Riesgos en dispositivos móviles. Suplantación de identidad (phishing): • Concepto. Tipos.	
INTEGRIDAD Y SEGURIDAD EN BASES DE DATOS.	27. Aplicar las diferentes operaciones sobre tablas en bases de datos desarrolladas.	• Identifica el procedimiento para la creación, administración y borrado de bases de datos. • Identifica la exploración de los elementos que conforman la minería de datos.	Entorno de trabajo del motor de bases de datos licenciado y de código abierto: Bases de datos: • Creación, modificación, administración y borrado. • Tablas. • Relaciones. • Registro Datos (Utilizando Lenguaje SQL con software licenciado y de código abierto). Minería de datos (Data Mining): • Conceptos. • Pasos para la minería de datos. Almacenes de datos (Big data).	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
			Principales características de la seguridad: • Elementos que pueden ser protegidos. • Arquitectura de seguridad de la información. • Niveles de seguridad en base de datos. Mecanismo de seguridad de la base de datos.	
OPERACIONES DE CIBERSEGURIDAD.	28. Explicar el papel en la empresa del analista de operaciones de ciberseguridad, y los recursos, características de los sistemas operativos necesarios parael análisis de ciberseguridad.	• Identifica los peligros y amenazas que se dan en las empresas en materia de ciberseguridad.	La ciberseguridad y los centrosde operaciones de seguridad: • Los peligros. • Actores de amenazas. • Impacto de la amenaza. • Guerra contra la ciberdelincuencia. • Centro de operaciones de ciberseguridad. Sistemas operativos. • Licenciados • De código abierto • Protección de los equipos	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
OPERACIONES DE CIBERSEGURIDAD.	29. Examinar el funcionamiento de los protocolos, servicios e infraestructuras de redes.	• Reconoce los dispositivosde comunicación por redes.	Protocolos y servicios de red • Protocolos de red • Ethernet y protocolo de Internet (IP) • Verificación de conectividad • Protocolo de resolución de direcciones • La capa de transporte • Servicios de red Infraestructuras de redes • Dispositivos de comunicación por redes • Infraestructura de seguridad de redes • Representaciones de redes	**2**
OPERACIONES DE CIBERSEGURIDAD.	30. Utilizar herramientas de monitoreo de redes y métodos que impidan el acceso malicioso a	• Diferencia las vulnerabilidades que pueden darse a las basesy a los servicios.	Monitoreo de red y herramientas • Topologías de seguridad de red • Métodos de monitoreo de red • Puntos de acceso de prueba de red	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
	datos, hosts y redes de computadoras.		• Analizadores de protocolos de red Ataque a las bases • Vulnerabilidades y amenazas de IP • Vulnerabilidades de TCP y UDP Ataques a los servicios • Servicios IP • Servicios empresariales • Defensa • Identificación de los activos • Identificación de vulnerabilidades • Control de acceso • Métodos y funcionamiento	
OPERACIONES DE CIBERSEGURIDAD.	31. Explicar el impacto de la criptografía sobre el monitoreo de la seguridad de redes, las	• Identifica el impacto de la criptografía sobre el monitoreo de la seguridad en las redes.	Criptografía • Integridad y autenticidad • Confidencialidad Criptografía de claves públicas • Autoridades y sistema de confianza • Aplicaciones e impactos	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
	vulnerabilidades de las terminales y los ataques.		Protección de terminales • Antimalware • Contra intrusiones con base en el host • Seguridad de aplicación Evaluación de vulnerabilidadesde terminales • Perfiles de redes y servidores • Sistemas de puntuación de vulnerabilidades • Marcos de trabajo para el cumplimiento • Administración segura de dispositivos • Análisis de datos	
SEGURIDAD EN EL INTERNET DE LAS COSAS (IOT)	32. Describir cómo el Internet de la cosas (IoT), los sistemas y arquitecturas, se enfrenta a riesgos y ataques y cómo	• Identifica los desafíos del Internet de las cosas (IoT).	El Internet de las cosas (IoT) bajo ataque • Internet de las cosas desafíos de seguridad • Cosas conectadas sin garantía • El riesgo único de IoT	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
	actuar ante estos desafíos.		• NICE e internet de las cosas • Casos de uso de seguridad de IoT • Caso de uso de IoT Sistemas y arquitecturas de IoT • Modelos de sistemas • Modelos de redes • Un modelo seguridad • Capas de seguridad • Requisitos de seguridad • Modelado de amenazas • Análisis del modelo de amenazas	
SEGURIDAD EN EL INTERNET DE LAS COSAS (IOT)	33. Analizar los ataques que se presentan a la capa física de los dispositivos de IoT.	• Identifica las vulnerabilidades y ataques en la capa de hardware.	• Ataque a la capa física de dispositivos IoT • Descripción general de los dispositivos IoT • Componentes de hardware del dispositivo IoT • Componentes de software del dispositivo de IoT	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
			• Vulnerabilidades y ataques en la capa de hardware • Seguridad de hardware • Vulnerabilidades de firmware • Mitigación de amenazas del dispositivo físico • Conceptos de control de acceso a la red • Cifrado	
SEGURIDAD EN EL INTERNET DE LAS COSAS (IOT)	34. Analizar los ataques que se presentan a la capa de aplicación de los dispositivos, evaluando las vulnerabilidadesy riesgos en el sistema de IoT	• Reconoce las vulnerabilidades en las aplicaciones locales, weby en la nube de los sistemas de IoT.	Ataques a la capa de aplicaciónde dispositivos IoT • Aplicación de IoT • Vulnerabilidades de la aplicación local de IoT • Vulnerabilidades en la aplicación web y en la nube de IoT • Protocolos de capa de IoT • Mitigación de problemas de seguridad en los protocolos de mensajería	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
			Evaluación de vulnerabilidades y riesgos en un sistema de IoT • Evaluación de vulnerabilidades y pruebas de penetración del sistema de IoT • Tipos y herramientas de prueba de vulnerabilidades • Riesgos con modelado de amenazas • Conceptos y enfoques. • Identificación y priorización de riesgos. • Gestión de riesgos en el sistema IoT • Innovaciones en seguridad de IoT • Introducción a blockchain Funcionamiento de blockchain	
ANÁLISIS AVANZADO DE CIBERSEGURIDAD	35. Describir las acciones que el analista de SOC tomaría con	• Identifica los roles y responsabilidades del analista de ciberseguridad.	Los roles y responsabilidades del analista de ciberseguridad • La InfoSec Wheel (Blue vs Purple vs Red)	**2**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

CIBERSEGURIDAD 2024

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
	compromiso en la operación de la red empresarial		• Roles de gestión, defensay ataque • Actores y amenazas • Guerra contra la ciberdelincuencia ¿Cómo organizar a tu equipo de ciberseguridad? • Protección de usuarios • Trazabilidad de los datos • Activos digitales Centro de Operaciones en Ciberseguridad SOC Arquitecturas de Ciberseguridad Manejo del riesgo informático • Liderazgo organizacional • Sistema de gestión de la Seguridad de la Información (SGSI) • Matriz de riesgo informático • Políticas y estándares	

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

Tema	Resultado de aprendizaje	Indicador de logro	Contenidos	N° ítems
ANÁLISIS AVANZADO DE CIBERSEGURIDAD	36. Utilizar las herramientas de red y orquestación para el monitoreo integral del ecosistema tecnológico.	• Reconoce los conceptosde red y herramientas de orquestración.	Monitoreo de red y herramientasde orquestación • Puntos de acceso de prueba de red. • Analizadores de protocolos de red. • Event logs • EDR • SIEM • SOAR	**1**

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr

ANEXO 1
GLOSARIO
DEFINICIÓN OPERACIONAL DE LOS VERBOS QUE SE UTILIZAN EN LOS OBJETIVOS DE ESPECIALIDADES TÉCNICAS:

IDENTIFICAR:

Definir conceptos. Determinar características y diferencias técnicas. Describir usos,requerimientos técnicos, funcionamientos y aplicaciones. Reconocer usos y aplicaciones. Clasificar categorías. Explicar procesos. Reconocer elementos que integran un todo. Distinguircomponentes y elementos que determinan un todo. Enumerar clases o tipos de componentesque forman un todo. Describir la diferencia entre datos e información. Explicar los conceptos, características y usos de las bases de datos. Reconocer la diferencia entre datos e información. Distinguir la función de los diferentes elementos de las bases de datos. Definir conceptos básicos relacionados con la estadística. Describir el proceso de investigación científica. Explicar diferentes etapas del proceso científico. Ejemplificar las técnicas para la recolección de datos. Identificar conceptos básicos relacionados con la estadística. Reconocer las etapas del proceso científico. Determinar técnicas para la selección de las fuentes de información. Explicar técnicas para la recolección de datos. Ejemplificar las técnicas para la interpretación de las medidas de posición. Utilizar las técnicas para la interpretación de las medidas de posición. Calcular las diferentes medidas de posición de acuerdo con los requerimientos de información. Definir conceptos básicos relacionados con el manejo de ventanas. Identificar los diferentes tipos de ventanas y tipos de cohesión de las ventanas. Describir los tipos de cohesión de ventanas por medio de ejemplos reales. Diseñar programassencillos que impliquen el manejo de ventanas. Definir conceptos relacionados con la interfazgráfica. Identificar el origen, funciones y características de la interfaz gráfica. Describir los diferentes criterios para el diseño de la interfaz gráfica. Ilustrar los diferentes criterios para el diseño

San José, Paseo Colón. Av. 1, calle 24, edificio Torre Mercedes, piso 7
Teléfono: (506)2547-5681 deac.dgec@mep.go.cr