Proceso Gestión de Formación Profesional Integral

Formato Planeación Pedagógica del Proyecto Formativo

Fecha de Elaboración	09/09/24
Denominación del Programa de Formación	TECNICO EN CONTROL DE LA SEGURIDAD DIGITAL
Modalidad de Ejecución	PRESENCIAL
Código y versión del Programa	233101
Nombre del Proyecto	FORTALECIMIENTO PEDAGÓGICO DE HABILIDADES DIGITALES PARA ESTUDIANTES Y PROFESIONALES INSTITUCIONES EDUCATIVAS Y EMPRESAS DEL DEPARTAMENTO DE CESAR
Código del Proyecto	2024
Instructor(es) que elabora la planeación pedagógica	**Nombres y Apellidos** EUSEBIO VARITH MACEA	**Regional y Centro de Formación** REGIONAL CAUCA-COMERCIO Y SERVICIOS

FASES DEL PROYECTO O ETAPAS DEL CICLO PROYECTO	ACTIVIDADES PROYECTO (Las mínimas requeridas)	COMPETENCIA	RESULTADOS DE APRENDIZAJE	APRENDIZAJES DE ADAPTABILIDAD Y MANEJO DE CAMBIO	HORAS/DIAS ACTIVIDADES DE APRENDIZAJE (DIRECTO)		HORAS TOTALES	HORAS DE LA GESTIÓN DE APRENDIZAJE (A + TEDA)	HORAS ORGANIZACIONALES OPCIONAL	AMBIENTE DE APRENDIZAJE REQUERIDO			DESCRIPCIÓN DE LA EVIDENCIA DE APRENDIZAJE	DESCRIPCIÓN DE LA EVIDENCIA APRENDIZAJE	OBSERVACIONES
					HORAS TRABAJO DIRECTO	HORAS TRABAJO INDEPENDIENTE				VIRTUAL	PRESENCIAL	TECNOLOGÍAS REQUERIDAS			
TRIMESTRE 1															
PLANEACIÓN		Aprovecha las diversas fuentes de información para la toma de decisiones.	Identifica fundamentos organizacionales del entorno, y las características básicas propias de la cuenca hidrográfica para la elaboración del proyecto.		24	14	38	1				Cuaderno, marcadores, tablero			
EJECUCIÓN	Aplicar la política de seguridad digital y resiliencia organizacional	Gestionar eventos relacionados con los riesgos de seguridad digital	Identifica la política de seguridad y privacidad de la información según el modelo de negocio	ambientes virtuales y medios de almacenamiento	76,8	19,2	96	2,00				Cuaderno, marcadores, tablero	Computadores, software de gestión de riesgos, internet, plataforma virtual		
		Diferenciar el origen, tipo y características de los diferentes riesgos de seguridad digital de acuerdo con la política de seguridad digital	Identifica información relevante para extraer los aspectos básicos de la política y de la norma ISO/IEC 27001		17,6	6,4	44	1,10							
			Describe características, definición y principales objetivos, intenciones y alcance de acuerdo con la normatividad y experiencia de vida		17,6	6,4	44	1,10							
			Identifica los diferentes tipos de riesgos de seguridad digital de acuerdo con la política de seguridad digital		17,6	6,4	44	1,10							
		Identificar el contexto interno y externo de acuerdo con principios claros para la administración del riesgo digital	Identifica los aspectos básicos de la política de seguridad y privacidad de la información		9,6	2,4	12	0,25							
			Describe los requerimientos identificados para el contexto interno y externo de la organización		9,6	2,4	12	0,25							
			Diferencia el contexto interno y externo de la organización		9,6	2,4	12	0,25							
			Identifica los requerimientos identificados para el contexto interno y externo de la organización		9,6	2,4	12	0,25							
	Proyecto: Fortalecimiento de habilidades en introducción de información para el Proceso Gestión Formación Profesional Integral	Clasificar activos, riesgos y vulnerabilidades según el modelo de negocio	Identifica los elementos y análisis de riesgos de seguridad de acuerdo con el modelo de negocio	Impacto de economías de escala para el control y análisis de riesgos tecnológicos.	38,4	9,6	48	1,00				Cuaderno, marcadores			
		Matemáticas	Identifica modelo económico de acuerdo con el análisis de riesgos de seguridad digital en contexto social y cultural		9,6	2,4	12	0,25							
			Realiza problemas matemáticos a partir de situaciones agrícolas en el contexto cotidiano		9,6	2,4	12	0,25							
			Plantea problemas matemáticos a partir de situaciones agrícolas en el contexto cotidiano		9,6	2,4	12	0,25							
			Plantea ejercicios de mayor nivel a los evaluados en pruebas saber 11 (prueba piloteada)		9,6	2,4	12	0,25							
		Utilizar herramientas de hardware y software de acuerdo con necesidades de usuario	Reconoce herramientas de hardware y software de acuerdo con necesidades de usuario		9,6	2,4	12	0,25				Cuaderno, marcadores, computadores, internet			
			Usa herramientas TIC de acuerdo con los requerimientos establecidos		9,6	2,4	12	0,25							
			Verifica las soluciones propuestas de acuerdo con los requerimientos		9,6	2,4	12	0,25							
			Implementa soluciones propuestas de acuerdo con los requerimientos establecidos		9,6	2,4	12	0,25							
		Diseñar soluciones para temas o situaciones específicas de acuerdo con los requerimientos y alcance	Identifica situaciones problemáticas susceptibles a ser resueltas de acuerdo con el contexto personal/comunidad/empresa		9,6	2,4	12	0,25							
			Plantea problemas y el alcance de acuerdo con los requerimientos y alcance		9,6	2,4	12	0,25							
			Interpreta problemas de acuerdo con el contexto		9,6	2,4	12	0,25							
			Verifica los resultados de los requerimientos establecidos		9,6	2,4	12	0,25							
		Total horas			403,2	100,8	504	12							
TRIMESTRE 2															
PLANEACIÓN	Implementar las políticas de seguridad digital y resiliencia de la información	Verificación de activos, riesgos y vulnerabilidades digital	Conoce el concepto de activo tecnológico, vulnerabilidad y riesgo de la información según el modelo de negocio y los controles básicos para su protección		110,4	9,6	120	2,50				Cuaderno, marcadores			
			Identifica el proceso de evaluación de incidentes según procedimientos establecidos para organización		110,4	9,6	120	2,50				Cuaderno, marcadores, computadores			
		Aplicación de metodologías de evaluación de riesgos	Valora la magnitud de la vulnerabilidad en relación con el riesgo de la información de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
			Identifica el impacto de la vulnerabilidad en relación con el riesgo de la información de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
			Propone soluciones de la vulnerabilidad en relación con el riesgo de la información de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
			Propone soluciones de la vulnerabilidad en relación con el riesgo de la información de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
		Selección de medios de tratamiento de riesgos	Identifica información relevante de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
			Identifica información apropiada para el tratamiento de riesgos de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
			Propone soluciones de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
			Implementa un plan de tratamiento de riesgos de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
	Identificar y monitorear los indicadores de seguridad	Protocolo de seguridad en la infraestructura digital	Aplica información de métodos de seguridad y privacidad de la información según el modelo de negocio		57,6	14,4	72	1,50				Cuaderno, marcadores			
			Implementa un modelo de seguridad y privacidad de la información según el modelo de negocio		57,6	14,4	72	1,50							
		Detección de fuentes de riesgos de seguridad digital	Detecta y sabe actividades de ingeniería social, fundamentos básicos de seguridad, tipos de ataques y técnicas para evitar, identificar el mismo de experiencia		25,6	6,4	32	0,67							
			Identifica las fuentes externas de riesgos de seguridad digital de acuerdo con el modelo de negocio		25,6	6,4	32	0,67							
			Propone planes de tratamiento de riesgos de seguridad digital de acuerdo con el modelo de negocio		25,6	6,4	32	0,67							
		Total horas			409,6	86,4	576	12							
TRIMESTRE 3															
EJECUCIÓN	Diseño y Desarrollo en seguridad digital	Controles de seguridad y resiliencia digital	Aplicar herramientas de control de la seguridad digital de acuerdo con el modelo de negocio y procedimientos internos de la empresa de seguridad digital		192	48	240	5,00				Cuaderno, marcadores			
		Gestionar procesos propios de la cultura organizacional para el fortalecimiento de la seguridad digital	Identifica aspectos básicos de la cultura organizacional y el contexto de ciudadanía		9,6	2,4	12	0,25							
			Diferencia la cultura de negocio de acuerdo con el modelo de negocio y procedimientos		9,6	2,4	12	0,25							
			Identifica el plan de negocio de acuerdo con el modelo de negocio y procedimientos		9,6	2,4	12	0,25							
			Valora la propuesta de negocio evidenciando el modelo de negocio y procedimientos		9,6	2,4	12	0,25							
		Aplicar de estrategias de seguridad digital en los procesos de innovación productiva social	Aplica fundamentos básicos de ética en la seguridad digital de acuerdo con el modelo de negocio/procedimientos de acuerdo con políticas		9,6	2,4	12	0,25							
			Identifica los aspectos que se pueden mejorar de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
			Diagnostica procesos de acuerdo con el modelo de negocio y procedimientos		9,6	2,4	12	0,25							
			Propone alternativas de mejora de los procesos de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
	Monitorear y documentar la gestión de incidentes y vulnerabilidades de seguridad digital	Controles de seguridad y resiliencia digital	Documentar incidentes de seguridad digital de acuerdo con el modelo de negocio y buenas prácticas		38,4	9,6	48	1,00				Cuaderno, marcadores			
		Desarrollar procesos de mejora continua de técnicas, tecnología y nuevos modelos de negocio digital	Identifica el contexto de la comunidad y sabe hacer un diagnóstico social, cultural,		9,6	2,4	12	0,25							
			Identifica las tecnologías emergentes para el fortalecimiento de la vida social y cultural,		9,6	2,4	12	0,25							
			Identifica los requerimientos de los procesos de innovación de acuerdo con el modelo de negocio y tecnología		9,6	2,4	12	0,25							
			Aplica estrategias de mejoramiento en el desarrollo de procesos comunitarios de acuerdo con el modelo de negocio		9,6	2,4	12	0,25							
		Total horas			345,6	86,4	432	9							