GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL
PROCEDIMIENTO DESARROLLO CURRICULAR
CRONOGRAMA

Cronograma de actividades

Guía de aprendizaje	Resultado de aprendizaje a alcanzar	Tipo de evidencia	Tiempos de entrega	
			Inicia	Termina
Actividades iniciales		Actualización de los datos personales.	1 de Abril	2 de Abril
		Respuestas al Sondeo de conocimientos previos.		
		Presentación ante el instructor y los compañeros en el Foro social.		
		Realización de la Actividad interactiva. Manejo de la plataforma.		
Actividad de aprendizaje 1: Reconocer las redes informáticas según las necesidades de sus requerimientos de seguridad.	**220501014-01:** Implementar la topología de red de la empresa de acuerdo con los niveles de seguridad requeridos por la misma y las políticas de seguridad a implantar.	**Evidencia:** Cuadro comparativo. Reconocer las diferentes topologías de redes y sus características.	2 de Abril	7 de Abril
		Evidencia: Protocolo. Desarrollar procesos de seguridad informática.		
Actividad de aprendizaje 2:		**Evidencia:** Mapa de cajas. Identificar los ataques más	8 de Abril	14 de Abril

Reconocer ataques informáticos teniendo en cuenta los diferentes tipos de redes.	**220501014-02:** Identificar los ataques más comunes a las empresas y plantear alternativas de solución de acuerdo con el conocimiento de las herramientas de control de acceso.	comunes a una red informática. **Evidencia:** Plegable. Determinar las políticas de protección contra ataques informáticos.		
Actividad de aprendizaje 3: Elaborar un manual de seguridad informática teniendo en cuenta las necesidades y características de la empresa.	**220501014-03:** Desarrollar un manual de seguridad informática de acuerdo con las necesidades, requerimientos y características de la empresa.	**Evidencia:** Mapa conceptual. Identificar los conceptos básicos para elaborar un manual de seguridad informática. **Evidencia:** Manual. Diseñar un manual de seguridad informática para una empresa.	15 de Abril	21 de Abril
Actividad de aprendizaje 4: Elaborar un plan de acción para evitar la pérdida de información de acuerdo con las políticas de seguridad establecidas en la empresa.	**220501014-04:** Desarrollar un plan de acción para implantar las políticas de seguridad informática en diversas jerarquías de la empresa.	**Evidencia:** Foro. Reconocer la importancia de las políticas de seguridad informática en una empresa. **Evidencia:** Actividad interactiva. Implantar las políticas de seguridad informática en una empresa. **Evidencia:** Plan de acción. Diseñar políticas de seguridad informática para una empresa.	22 de Abril	28 de Abril

		Respuestas al Sondeo de evaluación del programa.		