

LÍNEAS CURRICULARES: CONOCIMIENTOS BÁSICOS (DE ORIENTACIÓN TÉCNICA) ESPECIALIDAD TÉCNICA SOCIAL Y PERSONAL PRÁCTICA

PRIMER AÑO					SEGUNDO AÑO					3ER AÑO - 1ER SEMESTRE
CICLO 1	CICLO 2	CICLO 3	CICLO 4	CICLO 5	CICLO 6	CICLO 7	CICLO 8	CICLO 9	CICLO 10	SEMESTRE 1
MATEMÁTICA	ÁLGEBRA	FUNCIONES Y MATRICES						INGLÉS I	INGLÉS II	
	PROBABILIDAD Y ESTADÍSTICA	INFERENCIA ESTADÍSTICA								
	FUNDAMENTOS DE GESTIÓN	PROGRAMACIÓN	PROGRAMACIÓN ORIENTADA A OBJETOS	BASE DE DATOS RELACIONALES	PROGRAMACIÓN FRONT END	PROGRAMACIÓN BACK END	SEGURIDAD DE BASE DE DATOS	SEGURIDAD DE SISTEMAS OPERATIVOS	SEGURIDAD DE REDES	
			BASE DE DATOS	SISTEMAS OPERATIVOS	BASE DE DATOS NO ESTRUCTURADAS	LEGISLACIÓN Y CIBERSEGURIDAD		SERVICIOS CLOUD	SEGURIDAD DE SERVICIOS CLOUD	
			BASES DE HARDWARE Y SOFTWARE	FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN	METODOLOGÍA LEAN DISEÑO	INGENIERÍA DE SOFTWARES				
DESARROLLO DE HABILIDADES COMUNICACIONALES							TALLER DE LIDERAZGO Y EMPRENDIMIENTO			
										ACTIVIDADES DE TITULACIÓN
CURSO - TALLER PROPEDEÚTICO							ÉTICA SOCIAL Y PERSONAL			
								TALLER INTEGRACIÓN FULL STACK	TALLER INTEGRACIÓN EN SEGURIDAD DE DATOS Y REDES	PRÁCTICA LABORAL

CERTIFICACIONES INTERMEDIAS Las asignaturas marcadas con una letra conducen a la certificación del mismo color.

A CERTIFICADO EN CIBERSEGURIDAD Y PROTECCIÓN DE INFRAESTRUCTURAS

- » SEGURIDAD DE BASE DE DATOS
- » SISTEMAS OPERATIVOS
- » BASES DE HARDWARE Y SOFTWARE
- » FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

B CERTIFICADO EN DEFENSA CIBERNÉTICA Y RESPUESTA A INCIDENTES

- » SEGURIDAD DE BASE DE DATOS
- » SERVICIOS CLOUD
- » INGENIERÍA DE SOFTWARES

» Las mallas curriculares pueden ser actualizadas durante su desarrollo para un mejor proceso formativo.
» Esta malla no incluye los prerrequisitos de asignaturas.
» Existen asignaturas transversales que integran estudiantes de diferentes especialidades.

— ORIENTACIÓN DE LA CARRERA

La carrera de Técnico en Ciberseguridad entrega una sólida formación para desempeñarse en las prácticas y principios de la seguridad de la información. Capacita para desempeñar funciones críticas de protección, detección, respuesta y recuperación ante incidentes de seguridad informática, tanto en hardware como en software. Desarrolla habilidades prácticas en el manejo de herramientas de seguridad, análisis de vulnerabilidades, auditorías de sistemas y administración de medidas de protección cibernética, preparando a los titulados para enfrentar y mitigar efectivamente los riesgos digitales en las organizaciones. Esta formación se complementa con una actualización constante en las tendencias y tecnologías emergentes de seguridad, lo que posibilita a los titulados adaptarse rápidamente a un ambiente tecnológico en evolución y responder a las demandas del mercado laboral.

— PERFIL DE EGRESO

Él o la Técnico/a en Ciberseguridad del Instituto Profesional IPG posee una formación orientada hacia la aplicación práctica en el ámbito de la seguridad informática, con conocimientos sólidos en matemáticas, algoritmos, sistemas operativos, así como en la gestión y aseguramiento de la seguridad de redes y datos. Tiene la capacidad de implementar medidas de seguridad, realizar análisis de vulnerabilidades y aplicar protocolos de prevención y respuesta ante incidentes cibernéticos, colaborando en el diseño y fortalecimiento de la infraestructura de seguridad, contribuyendo a la protección de sistemas frente a amenazas digitales. Maneja herramientas de monitoreo de seguridad, realiza auditorías técnicas y apoya en la gestión de la continuidad del negocio. Su formación práctica le permite integrarse eficientemente a equipos multidisciplinarios y colaborar en el desarrollo de entornos tecnológicos seguros. Su formación valórica le permite desempeñar su trabajo de manera responsable y comprometida con la sociedad, respetuosa de la dignidad humana, basando su acción en el espíritu de emprendimiento, así como el respeto por la diversidad y mirada inclusiva.

— CAMPO OCUPACIONAL

Él o la Técnico/a en Ciberseguridad puede desempeñarse en organizaciones de distintos sectores, tales como financieros, comercio electrónico, industria tecnológica y entidades gubernamentales, y toda aquella que requiera la protección y gestión eficiente de su infraestructura cibernética. Puede ocupar posiciones de soporte en seguridad de la información, administración de sistemas de seguridad, monitoreo de redes y manejo de incidentes de ciberseguridad. Asimismo, puede ofrecer sus servicios de manera independiente realizando auditorías de seguridad, consultoría en protección de datos y en la implementación de estrategias de ciberdefensa ajustadas a las necesidades específicas de pequeñas y medianas empresas.