ANEXO

I. ESPECIFICACIÓN DE LA CARRERA

- **NOMBRE DE LA CARRERA:** *Tecnicatura Superior en Redes y Ciberseguridad*
- **TÍTULO QUE OTORGA:** *Técnico/a Superior en Redes y Ciberseguridad*
- **FAMILIA PROFESIONAL:** *Informática*
- **SUBSECTOR:** Software y Servicios Informáticos
- **CARGA HORARIA:** *2805 horas cátedra / 1870 horas reloj.*
- **MODALIDAD:** *Presencial / Bimodal*
- ***FORMATO DE LA CARRERA:*** *Disciplinar*
- **DURACIÓN:** *6 cuatrimestres*
- **CARÁCTER:** Diversificada y/o Especializada para las trayectorias profesionales previas de Informática o similares**.**
- **CONDICIONES DE INGRESO:**

Haber aprobado el Nivel Secundario o Ciclo Polimodal, o bien, ser mayor de 25 años según lo establecido en el Art. 7° de la Ley de Educación Superior N° 24.521 y cumplimentar lo establecido en la normativa provincial vigente.

PERFIL PROFESIONAL:

Competencias

Las competencias de un técnico en redes y ciberseguridad pueden variar dependiendo del contexto y el área específica en la que se desempeñe, sin embargo, algunas de las competencias más comunes incluyen:

- Conocimientos técnicos: Un técnico de esta especialidad debe conocer el mercado de tecnología de hardware informático, los avances en comunicaciones y redes nuevas tecnologías. Debe conocer además las vulnerabilidades existentes y la forma de mitigarlas.
- Habilidades de resolución de problemas: Los técnicos en informática deben ser capaces de investigar, identificar y resolver problemas de manera efectiva.
- Habilidades de comunicación: Es importante que los técnicos sean capaces de comunicarse de manera clara y efectiva tanto con los equipos de trabajo como con los clientes.
- Habilidades de colaboración: Los técnicos, generalmente, trabajan en equipos interdisciplinarios, por lo que es importante que sean capaces de colaborar y trabajar de manera efectiva con otros miembros del equipo, entendiendo los alcances de cada una de las disciplinas.

- Habilidades de aprendizaje continuo: La tecnología está en constante evolución, por lo que es importante que los técnicos estén dispuestos a aprender y a mantenerse actualizados con las últimas tendencias y tecnologías.
- Conocimientos de metodologías ágiles: Trabajar en forma colaborativa con distintos equipos de trabajo. Gestionando las actividades propias y del equipo.

Competencias Profesionales

- Administrar servidores, software de base, comunicaciones y demás subsistemas, maximizando el aprovechamiento de los recursos y anticipando posibles problemas.
- Manejar incidentes que afecten a la Infraestructura de TI, diagnosticando las causas que los originan y resolviendo o coordinando las acciones para su solución.
- Instalar o reemplazar componentes de la Infraestructura de TI o adaptarla a nuevas condiciones de servicios externos minimizando riesgos para la seguridad y continuidad del servicio.
- Asesorar en la compra de nueva infraestructura.
- Desarrollar en forma sinérgica y creativa el liderazgo, la comunicación activa y el trabajo en equipo, en los múltiples ámbitos de desempeño que plantea el mundo laboral.

Competencia general 1: Administrar servidores, software de base, comunicaciones y demás subsistemas, maximizando el aprovechamiento de los recursos y anticipando posibles problemas.

1.1.

Actividades	Criterios de realización
a) Monitorear la distribución de carga de los sistemas y el uso de los recursos que componen la infraestructura.	• Se define y utiliza software para el control de carga y dimensionamiento de la infraestructura. • Se crean scripts que generan alarmas de sobre - dimensionamiento o mal funcionamiento de recursos.

1.2.

Actividades	Criterios de realización

a) Garantizar la seguridad de la instalación.	• Se analiza la disposición y control de acceso a la planta informática. • Se proponen planes de mejora para asegurar los recursos físicos de la planta informática. • Se controlan los dispositivos de seguridad física y lógica. • Se realizan test de intrusión para garantizar la seguridad.

1.3.

Actividades	Criterios de realización
a) Administrar medios masivos de almacenamiento.	• Se analizan los espacios libres de los sistemas de almacenamiento masivo, adecuando las capacidades o eliminando información superflua. • Se realizan informes de crecimiento evolutivo del almacenamiento para asegurar el correcto dimensionamiento del mismo. • Se proponen planes de mejora para asegurar los recursos físicos de la planta informática.

1.4.

Actividades	Criterios de realización
a) Administrar permisos de acceso a los sistemas.	• Se otorgan roles de usuarios y permisos asociados a cada sistema. • Se configuran las reglas de acceso de firewalls y las políticas de usuario del S.O.

1.5.

Actividades	Criterios de realización
a) Implementar cambios o aplicar parches en software de base.	• Se verifican las versiones y actualizaciones disponibles del software base, instalado. • Se instalan versiones o mejoras propuestas por los proveedores.

1.6.

Actividades	Criterios de realización

a) Actualizar instalaciones informáticas.	• Se solicitan y evalúan presupuestos a proveedores externos para adecuar planes de actualización o reparación. • Se ejecutan planes de actualización del equipamiento.

1.7.

Actividades	Criterios de realización
a) Administrar backups y automatizaciones.	• Se realizan respaldos de información periódicos en forma programada, automatizada y monitoreada.

1.8.

Actividades	Criterios de realización
a) Planificar la evolución de la capacidad disponible	• Se analizan y proponen planes de actualización para asegurar el crecimiento evolutivo de los recursos necesarios en la planta informática.

***Competencia general 2*:** Manejar incidentes que afecten a la Infraestructura de TI, diagnosticando las causas que los originan y resolviendo o coordinando las acciones para su solución.

2.1.

Actividades	Criterios de realización
a) Identificar causas de incidentes.	• Se interpretan las causas que originan el problema. • Se diagnostica el origen del mismo. • Se establece un orden de prioridades para implementar soluciones.

2.2.

Actividades	Criterios de realización
a) Planificar las acciones necesarias para resolver el problema.	• Se desarrollan estrategias de solución. • Se ejecutan las tareas de reparación minimizando el tiempo de parada. • Se derivan las acciones de solución (de ser necesario).

2.3.

Actividades	Criterios de realización

a) Verificar que la solución implementada haya resuelto el problema.	• Se ejecutan testeos de funcionamiento para garantizar la resolución de los incidentes.

Competencia general 3: Instalar o reemplazar componentes de la Infraestructura de TI o adaptarla a nuevas condiciones de servicios externos minimizando riesgos para la seguridad y continuidad del servicio.

3.1.

Actividades	Criterios de realización
a) Requerir presupuestos para adecuaciones o nuevas instalaciones.	• Se solicitan y seleccionan presupuestos de diversos proveedores.

3.2.

Actividades	Criterios de realización
a) Reemplazar e instalar componentes de hardware o redes.	• Se analizan especificaciones técnicas de los nuevos componentes y requerimientos de funcionamiento de los mismos. • Se evalúa la compatibilidad y posibilidad de expansión. • Se planifica el orden y prioridad de instalación, verificando el impacto sobre la planta actual. • Se solicitan y seleccionan presupuestos de diversos proveedores. • Se realiza la instalación, ejecutando planes de prueba y asegurando el correcto funcionamiento del mismo.

3.3.

Actividades	Criterios de realización

a) Reemplazar o instalar versiones de software de base o aplicaciones.	• Se interpreta la documentación técnica del software o aplicación requerida. • Se verifica que los componentes instalados cumplan el rol para el que se programaron. • Se instalan componentes de software para garantizar el funcionamiento de las aplicaciones. • Se realizan pruebas integrales para garantizar la funcionalidad y seguridad de las actualizaciones propuestas.

3.4.

Actividades	Criterios de realización
a) Preparar backups de los componentes modificados.	• Se realizan respaldos del software o de los componentes reemplazados. • Se planifica plan de contingencia para la recuperación de los mismos en caso de falla en la modificación.

3.5.

Actividades	Criterios de realización
a) Elaborar la documentación actualizada sobre el layout físico y lógico de las distintas plataformas y la Infraestructura de TI.	• Se confeccionan documentos técnicos para garantizar la trazabilidad de los cambios. • Se realizan o modifican planos de infraestructura y cableado.

Competencia general 4**:** Asesorar en la compra de nueva infraestructura.

4.1.

Actividades	Criterios de realización
a) Actualizarse sobre tendencias y nuevas incorporaciones.	• Se verifican frecuentemente las publicaciones especializadas del rubro informático, que puedan mejorar o actualizar la planta instalada.

4.2.

Actividades	Criterios de realización
a) Realizar análisis del mercado regional sobre oferta, disponibilidad y soporte.	• Se consideran las nuevas tendencias y productos del mercado informático local. • Se asesora cuáles son los mejores productos a adquirir.

4.3.

Actividades	Criterios de realización
a) Evaluar la calidad de los proveedores.	• Se evalúan los potenciales proveedores dependiendo de cada producto. • Se confecciona un reporte de características o cualidades de cada proveedor que ayude a la toma de decisiones para la adquisición de un producto.

Competencia general 5: Desarrollar en forma sinérgica y creativa el liderazgo, la comunicación activa y el trabajo en equipo, en los múltiples ámbitos de desempeño que plantea el mundo laboral.

5. 1.

Actividades	Criterios de realización
a) Favorecer procesos activos de intercomunicación.	• Se desarrolla la escucha activa. • Se discuten los temas de forma personal, uno a uno. • Se producen diálogos constantes, sin caer en la acumulación de opiniones negativas. • Se prioriza la especificidad, evitando generalizaciones en el diálogo. • Se desarrollan momentos de comunicación grupal para encontrar dinamismo en el grupo de trabajo.

5. 2.

Actividades	Criterios de realización
a) Conformar equipos de trabajo dinámicos.	• Se favorece el desarrollo de interacciones grupales colaborativas.

5. 3.

Actividades	Criterios de realización
a) Capacidad creativa para la resolución de situaciones problemáticas.	• Se afronta de forma crítica cada situación problema. • Se analiza la situación, ya sea de forma inductiva o deductiva. • Se proponen soluciones que consideren todos los puntos conflictivos de la problemática. • Se consideran distintos tipos de seguimiento para la concreción de la solución.

5. 4.

Actividades	Criterios de realización
a) Promover el desarrollo de proyectos dentro y fuera de la organización.	• Se desarrollan vinculaciones con el contexto internacional, nacional y regional. • Se fomenta la generación de capacidades emprendedoras para ser aplicadas en los diferentes ámbitos de concreción. • Se consideran diferentes estructuras de proyectos.

V. COMPONENTES CURRICULARES

1. Organización curricular por campos de formación

Campos	Nombre	Régimen de Cursado	Horas cátedra anuales	Horas reloj anuales
GENERAL	Inglés técnico I	Anual	120	80
	Alfabetización Académica	Cuatrimestral	60	40
	Legislación Informática y Ética profesional	Cuatrimestral	45	30
	Auditoría de Seguridad Informática	Cuatrimestral	45	30
Subtotal			**270**	**180**
% del Campo				**9,6**
DE FUNDAMENTO	Matemática Aplicada	Anual	90	60
	Lógica Computacional	Anual	90	60
	Arquitectura de Dispositivos	Cuatrimestral	45	30
	Seminario Nuevas Tecnologías	Cuatrimestral	45	30
	Matemática Aplicada II	Anual	90	60
	Inglés técnico II	Anual	120	80
	Inglés técnico III	Anual	120	80

Subtotal			**600**	**400**
% **del Campo**				**21,4**
ESPECÍFICO	Programación I	Anual	180	120
	Sistemas Operativos I	Cuatrimestral	45	30
	Base de Datos I	Anual	90	60
	Mantenimiento de Instalaciones Informáticas	Cuatrimestral	90	60
	Higiene y Seguridad Informática	Cuatrimestral	45	30
	Administración de Servidores	Anual	120	80
	Comunicación y Redes	Cuatrimestral	90	60
	Taller de Instalación y Certificación de Redes	Cuatrimestral	60	40
	Criptografía Aplicada	Cuatrimestral	45	30
	Automatización de Servicios Informáticos	Cuatrimestral	60	40
	Electrónica Aplicada	Cuatrimestral	60	40
	Tecnología IoT	Cuatrimestral	60	40
	Tratamiento de Incidentes de Continuidad de Negocio	Cuatrimestral	60	40
	Videovigilancia y Control de Accesos	Cuatrimestral	60	40
	Ciberseguridad	Anual	180	120
	Investigación Digital y Cibercrimen	Cuatrimestral	75	50
	Forense Digital	Cuatrimestral	75	50
	Ethical Hacking	Anual	90	60
Subtotal			**1485**	**990**
% **del Campo**				**53**
	Práctica Profesionalizante I	Anual	120	80
	Práctica Profesionalizante II	Anual	150	100
	Práctica Profesionalizante III	Anual	180	120
Subtotal			**450**	**300**
% **del Campo**				**16**
Total de horas			**2805**	**1870**

2. Distribución de espacios curriculares por año.

PRIMER AÑO

1° Cuatrimestre					**2° Cuatrimestre**				
Unidad Curricular		**Formato**	**HC**	**HCT**	**Unidad Curricular**		**Formato**	**HC**	**HCT**
Cód.	**Denominación**				**Cód.**	**Denominación**			
1	Programación I	TA	6		1	Programación I	TA	6	180

2	Matemática Aplicada	A	3		2	Matemática Aplicada	A	3	90
3	Lógica Computacional	M	3		3	Lógica Computacional	M	3	90
4	Inglés técnico I	T	4		4	Inglés técnico I	T	4	120
5	Alfabetización académica	T	4	60	6	Seminario Nuevas Tecnologías	S	3	45
7	Arquitectura de Dispositivos	M	3	45	8	Sistemas Operativos I	M	3	45
9	Base de Datos I	T	3		9	Base de Datos I	T	3	90
10	Práctica Profesionalizante I	pp	4		10	Práctica Profesionalizante I	PP	4	120
Total de horas Cátedra 1° Cuatrimestre			**30**		**Total de horas Cátedra 2° Cuatrimestre**			**29**	
Total de horas cátedra de Primer Año									**885**
Total de horas reloj de Primer Año									**590**

SEGUNDO AÑO

1° Cuatrimestre					**2° Cuatrimestre**				
Unidad Curricular		**Formato**	**HC**	**HCT**	**Unidad Curricular**		**Formato**	**HC**	**HCT**
Cód.	**Denominación**				**Cód.**	**Denominación**			
11	Mantenimiento de Instalaciones Informáticas	T	6	90	**12**	Higiene y Seguridad Informática	M	3	45
13	Matemática Aplicada II	M	3		**13**	Matemática Aplicada II	M	3	90
14	Administración de Servidores	M	4		**14**	Administración de Servidores	M	4	120
15	Inglés Técnico II	T	4		**15**	Inglés Técnico II	T	4	120
16	Comunicación y Redes	M	6	90	**17**	Taller de Instalación y Certificación de Redes	M	4	60
18	Criptografía Aplicada	M	3	45	**19**	Automatización de Servicios Informáticos	T	4	60
20	Electrónica Aplicada	T	4	60	**21**	Tecnologías IoT	T	4	60
22	Práctica Profesionalizante II	PP	5		**22**	Práctica Profesionalizante II	PP	5	150
Total de horas Cátedra 1° Cuatrimestre			**35**		**Total de horas Cátedra 2° Cuatrimestre**			**31**	
Total de horas cátedra de Segundo año									**990**
Total de horas reloj de Segundo año									**660**

TERCER AÑO

1° Cuatrimestre					2° Cuatrimestre				
Unidad Curricular		**Formato**	**HC**	**HCT**	**Unidad Curricular**		**Formato**	**HC**	**HCT**
Cód.	**Denominación**				**Cód.**	**Denominación**			
23	Tratamiento de Incidentes de Continuidad de Negocio	T	4	60	**24**	Videovigilancia y Control de Accesos	T	4	60
25	Ciberseguridad	M	6		**25**	Ciberseguridad	M	6	180
26	Inglés Técnico III	T	4		**26**	Inglés Técnico III	T	4	120
27	Legislación Informática y Ética Profesional	A	3	45	**28**	Auditoría de Seguridad Informática	A	3	45
29	Investigación Digital y Cibercrimen	T	5	75	**30**	Forense Digital	T	5	75
31	Ethical Hacking	T	3		**31**	Ethical Hacking	T	3	90
32	Práctica Profesionalizante III	PP	6		**32**	Práctica Profesionalizante III	PP	6	180
Total de horas Cátedra 1° Cuatrimestre			**31**		**Total de horas Cátedra 2° Cuatrimestre**			**31**	
Total de horas cátedra de tercer año									**930**
Total de horas reloj de tercer año									**620**
Total de horas cátedra de la carrera									**2805**
Total de horas reloj de la carrera									**1870**

3. Trayectorias Formativas para Certificaciones Intermedias Formación Profesional de Nivel 3 (FP3).

Denominación: Administrador de Redes e Infraestructura Tecnológica

3.1. Perfil profesional de la Certificación

1. Instalar, mantener y actualizar productos de tecnologías de la información que cumplen funciones de sistema operativo, administración de almacenamiento, comunicaciones y redes, seguridad, bases de datos y otros subsistemas, para garantizar la máxima disponibilidad del ambiente operativo de las aplicaciones informáticas de las organizaciones. Interactuar calificadamente con profesionales de otros campos, desempeñándose en forma autónoma o en relación de dependencia. Estará en condiciones de cumplir las siguientes funciones:
    1.1. Instalar y realizar la puesta en funcionamiento de productos de tecnología de la información que cumplen funciones de sistema operativo, comunicaciones y redes de datos, almacenamiento de datos, seguridad informática, base de datos y otros subsistemas. Para ello:

- Instala productos de tecnologías de la información: sistemas operativos, dispositivos de red (por ejemplo, computadores, impresoras IP, cámaras de video IP, teléfonos IP), módems, conmutadores, enrutadores y servidores.
- Establece los parámetros de funcionamiento que el producto de tecnología requiera para satisfacer las necesidades exigidas.
- Configura el software de los productos instalados. Verifica el correcto funcionamiento de los productos instalados.

1.2. Administrar productos de tecnología de la información que cumplen funciones de sistema operativo, comunicaciones y redes de datos, almacenamiento de datos, seguridad informática, base de datos y otros subsistemas. Para ello:

- Contribuye a la definición y el mantenimiento de la accesibilidad de los servicios y la optimización de los recursos.
- Monitorea la distribución de carga del sistema y el uso de los recursos que componen la infraestructura.
- Administra permisos a usuarios de sistemas y subsistemas.
- Automatiza operaciones rutinarias y/o previsibles.

1.3. Mantener productos de tecnología de la información que cumplen funciones de sistema operativo, comunicaciones y redes de datos, almacenamiento de datos, seguridad informática, base de datos y otros subsistemas. Para ello:

- Atiende incidentes que afecten a la infraestructura de tecnología de la información, diagnosticando sus causas y resolviéndolas, o coordinando su solución garantizando la seguridad y la continuidad del servicio.
- Actualiza sistemas, aplicaciones o datos, incluyendo actualización de sistemas operativos y migración a distintos tipos de accesos a internet.
- Reemplaza componentes de la infraestructura de tecnología de la información, tales como sistemas operativos, sistemas dedicados, terminales de hardware, periféricos, conmutadores, enrutadores y/o medios de almacenamiento.
- Elabora y ejecuta procedimientos de optimización y mantenimiento preventivo de la infraestructura de la tecnología de la información a fin de minimizar riesgos para la seguridad y continuidad del servicio.
- Monitorea el tráfico, actualiza los layouts físico y lógico, reasigna recursos cuando corresponda, manteniendo el parque electrónico de la red, el cableado y los vínculos asociados.
- Interviene en temas de contingencias y riesgos que puedan afectar a la infraestructura de tecnología de la información.

1.4. Asistir a los usuarios de redes de computadoras en lo referido al uso correcto de las mismas y dar solución a aspectos técnicos no previstos.

1.5. Asesorar técnicamente en relación con la incorporación de productos de tecnología de la información que cumplen funciones de sistema operativo, comunicaciones y redes de datos, almacenamiento de datos, seguridad informática, base de datos y otros subsistemas. Para ello:

- Realiza estudios y análisis comparativo de las características técnicas y operativas de los productos de tecnología de la información ofrecidos en el mercado.
- Interviene en las distintas etapas técnicas de un proceso de compras de productos de tecnología de la información.
- Realiza el análisis de prefactibilidad técnica y económica de los productos a incorporar.

1.6. Desarrollar proyectos que se relacionen con productos de tecnología de la información y que cumplen funciones de sistema operativo, comunicaciones y redes de datos, almacenamiento de datos, seguridad informática, base de datos y otros subsistemas. Para ello:

- Diseña sistemas de redes de comunicaciones de datos, incluyendo el dimensionamiento, la elección de la topología de la red, el direccionamiento IP de la red y subredes asociadas y la configuración de enrutadores y conmutadores de acuerdo a las necesidades.
- Realiza el análisis de la prefactibilidad técnica y económica de emprendimientos productivos en el ámbito de las tecnologías de la información.

1.7. Producir documentación técnica vinculada con las tareas desarrolladas.

1.8. Participar en la política de seguridad informática sugiriendo criterios de protección al ingreso de usuarios no autorizados e implementándolos.

3.2. Componentes curriculares de la certificación:

Designación de certificación Intermedia	Espacios Curriculares	HC
Administrador de Redes e Infraestructura Tecnológica	Programación I	180
	Matemática Aplicada	90
	Lógica Computacional	90
	Inglés Técnico I	120
	Alfabetización Académica	60
	Arquitectura de Dispositivos	45
	Sistemas Operativos I	45
	Bases de Datos I	90
	Seminario Nuevas Tecnologías	45
	Práctica Profesionalizante I	120
	Mantenimiento de Instalaciones Informáticas	90

	Higiene y Seguridad Informática	45
	Inglés Técnico II	120
	Comunicación y Redes	90
	Taller de Instalación y Certificación de Redes	60
	Administración de Servidores	120
	Electrónica Aplicada	60
	Tecnologías IoT	60
	Práctica Profesionalizante II	150
Carga Horaria Total		**1680**

3.3. Requisitos para la certificación de la trayectoria

Se otorgará la certificación correspondiente a los estudiantes que acrediten los espacios curriculares de la trayectoria y que a través de un trabajo integrador final específico al cierre del proceso demuestren haber logrado las competencias definidas por perfil Profesional.

El trabajo integrador específico deberá surgir de las prácticas profesionalizantes I y II y deberá ser inherente a la certificación otorgada.

En la dicha instancia de acreditación deberán constituirse un tribunal evaluador integrado por el coordinador de la carrera y un profesor por cada campo de formación (general, fundamento, específica y práctica profesionalizante).

4. DESCRIPTORES POR ESPACIO CURRICULAR

PRIMER AÑO

1 - PROGRAMACIÓN I

Concepto de algoritmo, resolución algorítmica de problemas, estrategias de diseño, de implementación, de depuración. Algoritmos fundamentales, algoritmos numéricos simples. Estructuras fundamentales, variables, tipos, expresiones y asignaciones, entrada/salida, estructuras de control condicionales e iterativas, funciones y pasaje de parámetros, descomposición estructurada.

Concepto de lenguaje de alto nivel y la necesidad de traducción, comparación entre compiladores e intérpretes, aspectos de la traducción dependientes y no dependientes de la máquina. Máquinas virtuales, concepto, jerarquía de máquinas virtuales, lenguajes intermedios, asuntos de seguridad que surgen al ejecutar código en una máquina diferente. Representación de datos numéricos, rango, precisión y errores de redondeo. Arreglos. Representación de datos de caracteres, listas y su procesamiento.

Programación modular: Concepto. Aplicación: estructura de un programa utilizando

procedimientos y funciones. Reglas para escribir algoritmos eficientes. Elaboración de "algoritmos-tipo" o estándar a partir de métodos lógicos matemáticos, por ejemplo: uso de funciones matemáticas recursivas, funciones recursivas simples, búsqueda sucesiva y binaria y de ordenamiento. Algoritmos de camino mínimo. Elementos de complejidad de algoritmos. Pruebas de escritorio para validar algoritmos. Verificación unitaria de unidades de código, concepto de cubrimiento, organización, ejecución y documentación de la prueba**.**

Desarrollo de Programas Ambientes de programación. Introducción al uso de librerías y APIs (interfaz de programación de aplicaciones). Lenguaje de programación: Estructura sintáctica de un programa en el lenguaje de aplicación. Reglas sintácticas del lenguaje. Sintaxis de procedimientos y funciones. Reglas del lenguaje.

Programación Web Básica Fundamentos de la programación web: HTML, CSS y JavaScript. Creación y estructuración de páginas web utilizando HTML. Estilos y diseño de páginas web con CSS. Interactividad en páginas web con JavaScript. Desarrollo de formularios y validación de datos. Introducción a las bibliotecas y frameworks de JavaScript. Buenas prácticas en el desarrollo web. Pruebas y depuración de aplicaciones web.

2 – MATEMÁTICA APLICADA

Matrices y Determinantes. Conjuntos numéricos. Matrices. Concepto de matriz. Dimensión de una matriz. Tipos de matrices: matriz fila, matriz columna, matriz cuadrada, matriz rectangular, matriz diagonal, matriz simétrica. Igualdad de matrices. Operaciones con matrices. Determinantes: La función determinante, matriz inversa, rango. Espacio Vectorial. Vectores de n componentes. Generalización. Operaciones internas y externas, normas, proyecciones, dependencia lineal, base y dimensión. Adición y sustracción de vectores. Producto de un vector por un escalar. Producto escalar.

Sistema de ecuaciones. Clasificación. Teorema de Roché Frobenius, resolución. Expresión matricial de un sistema ecuaciones lineales con N incógnitas. Sistemas equivalentes. Resolución de sistemas de ecuaciones. Compatibilidad de los sistemas. Sistemas homogéneos. Operaciones internas y externas, norma, proyecciones, dependencia lineal, base y dimensión. Aplicaciones de los espacios vectoriales. Transformaciones lineales: teorema fundamental, matriz asociada, autovalores y autovectores, diagonalización.

3 – LÓGICA COMPUTACIONAL

Lógica proposicional. Elementos de lógica. Lógica proposicional, conectivos lógicos. Formas normales: conjuntiva y disyuntiva. Validez. Adquisición del conocimiento, forma del conocimiento, uso del conocimiento, límites del conocimiento. Intratabilidad e inexpresabilidad. Enunciados y conectivas. Funciones de verdad y tablas de verdad. Argumentación y validez. Lógica de Enunciados. Reglas de manipulación y sustitución. Formas normales. Conjuntos adecuados de

conectivas.
Lógica de predicados. Lógica de predicados, cuantificadores: Universal y existencial. Limitaciones de la lógica de predicados- Lenguajes de primer orden. Interpretaciones Satisfacción y verdad. El sistema formal. Corrección y completitud. Modelos de sistemas de primer orden.
Lógica digital. Introducción a la Lógica digital, Álgebra de Boole, Compuertas lógicas: NAND (No Y), NOR (No O), OR exclusiva (O exclusiva). Multiplexores, decodificadores, biestables, memorias, microcontroladores, microprocesadores. Funciones. Método de Kamaugh

4 – INGLÉS TÉCNICO I

Los siguientes descriptores deberán abordarse desde las cuatro macro-habilidades (comprensión lectora y auditiva y producción escrita y oral) y orientarse al campo de desempeño del futuro profesional, desarrollando las competencias básicas fijadas por los estándares del Marco Común Europeo de Referencia para la competencia lingüística de nivel A1: al finalizar el cursado, el estudiante será capaz de comprender y utilizar expresiones cotidianas de uso muy frecuente así como frases sencillas destinadas a satisfacer necesidades de tipo inmediato. podrá presentarse a sí mismo y a otros, pedir y dar información personal básica sobre su domicilio, sus pertenencias y las personas que conoce. Podrá relacionarse de forma elemental siempre que su interlocutor hable despacio y con claridad y esté dispuesto a cooperar.
Contenidos mínimos:
El estudiante deberá desarrollar habilidades de producción (habla y escritura) aplicadas a situaciones específicas de la carrera y el año que transita.
Preguntas abiertas. Preguntas cerradas. Sustantivos y adjetivos posesivos. Verbo be. Preposiciones de tiempo y lugar. Preferencias con would like. Presente simple. There is y there are. Sustantivos contables e incontables. Artículos definido e indefinido. Presente continuo. Verbos modales. Pasado simple. Adjetivos comparativos y superlativos. Futuro con be going to.

5 – ALFABETIZACIÓN ACADÉMICA

Competencia comunicativa. La comunicación: definición, elementos de la situación comunicativa. Funciones del lenguaje. El contexto: adecuación del texto al contexto. Registro. Objetividad y subjetividad en el mensaje. Tipos de comunicación. Concepto de texto. Concepto de discurso. Propiedades de los textos: adecuación, coherencia, cohesión y normativa. Tipologías textuales. Texto explicativo-expositivo. Texto argumentativo. Texto instructivo. Correcta redacción de prompts de IA, preguntas y respuestas en bots, y lenguajes de tipo low-code más textuales.
La comprensión lectora: estrategias y fases. El resumen/síntesis. Producción de Textos: planificación, textualización y revisión. Informe. Textos instrumentales. La intencionalidad comunicativa: persuasión e información. Reconocimiento de ideas nucleares y periféricas. Elaboración de esquemas: jerárquicos – cronológicos – comparativos. Indicadores de

autoevaluación.

Introducción al procesamiento de lenguaje natural (PLN), relación con la inteligencia artificial. Importancia de la claridad y precisión en la redacción de prompts para obtener respuestas adecuadas. Estrategias para adaptar el tono y estilo según el contexto, junto con técnicas para identificar y corregir problemas en la interpretación de prompts por parte de la IA. Evaluación de prompts y consideraciones éticas para evitar sesgos en la interacción con herramientas de IA.

Capacidad de aprender a aprender. Learn agility. Definiciones. La necesidad del aprendizaje continuo en los tiempos del Agilisimo y la digitalización. Aprender a re Aprender. Contexto VUCA. Contexto BUNI. Aprendizaje y trabajo. Upskilling. Reskilling. Estilos de aprendizaje. Actitudes del aprendiz. Aprender a ser aprendiz. Mejorar la capacidad de aprender. Inteligencia interpersonal e intrapersonal. Inteligencia emocional. Herramientas para desarrollar la Learnability individual. Rasgos clave. Activar el proceso de Aprendizaje Ágil. Capacidad de aprender sobre el error. Experimentar. Gestión del feedback: pedido y escucha. Gestión de la motivación intrínseca.

6 – SEMINARIO NUEVAS TECNOLOGÍAS

Inteligencia Artificial. Introducción a la ciencia de datos e inteligencia artificial. Relevancia de la IA en el desarrollo de software y la ciberseguridad. Herramientas populares: GitHub Copilot, TabNine, ChatGPT. IA en la Seguridad del Software. Detección de vulnerabilidades y amenazas. Implementación de medidas de seguridad basadas en IA.

Introducción a las Redes de Computadoras. Comprender los conceptos fundamentales de las redes de computadoras. Aprender sobre IP, puertos y DNS. Realizar configuraciones básicas de red en una computadora. Configuración de IP estática y dinámica. Configuración de DNS en una computadora. Uso de comandos de red básicos (ping, ipconfig/ifconfig, nslookup).

Introducción a Bases de Datos Relacionales. Comprender los conceptos fundamentales de las bases de datos relacionales. Aprender a crear y relacionar tablas en una base de datos. Realizar consultas básicas utilizando SQL. Definición y tipos de bases de datos. Modelos de bases de datos relacionales. Creación y Gestión de Tablas: Definición de entidades y atributos. Creación de tablas en SQL. Relaciones entre tablas (claves primarias y foráneas). Consultas Básicas en SQL: Insertar, actualizar y eliminar datos. Consultas básicas: SELECT, WHERE, JOIN.

7 – ARQUITECTURA DE DISPOSITIVOS

Sistemas numéricos de distintas bases, operaciones básicas, resta por complemento, circuitos lógicos y digitales básicos, códigos y representaciones. Tecnología: memorias, almacenamientos auxiliares, dispositivos de entrada y salida. Unidad Central de Procesamiento (CPU). Estructura y funcionamiento de la CPU. Memoria. Tipos de memoria: RAM, ROM, Cache.

Jerarquía de memoria. Funcionamiento de la memoria virtual. Sistemas de Almacenamiento. Discos duros (HDD) y unidades de estado sólido (SSD). Sistemas de archivos y gestión de

almacenamiento. Buses de Datos y Direcciones Unidades de Entrada y Salida (E/S). Bloque Arquitectura Interna de la CPU y Sistemas de Memoria. Arquitectura Interna de la CPU. Registro y ALU (Unidad Aritmética Lógica). Tipos de registros. Funcionamiento de la ALU. Unidad de Control. Sistemas de memoria. Memoria caché. Memoria principal.

Simulación de Arquitectura y Montaje. Introducción a BLUE y Simulación de Arquitectura. Instalación y configuración de BLUE. Interfaz de usuario de BLUE. Simulación de arquitectura de computadoras con BLUE. Prácticas con BLUE. Montaje y desmontaje de un dispositivo. Identificación y descripción de componentes físicos.

8 – SISTEMAS OPERATIVOS I

Fundamentos. Introducción a los sistemas operativos. Historia y evolución de los sistemas operativos. Funciones y componentes de un sistema operativo. Tipos de sistemas operativos. Arquitectura de sistemas operativos. Gestión de procesos: Estados de un proceso. Planificación de procesos. Hilos y multitarea. Gestión de memoria: Jerarquía de memoria. Memoria principal y secundaria. Memoria virtual. Técnicas de asignación y paginación. Sistemas de archivos: Estructura y organización de sistemas de archivos. Tipos de sistemas de archivos. Operaciones sobre sistemas de archivos. Gestión de dispositivos: Controladores de dispositivos. Gestión de entradas y salidas (E/S).

Administración. Instalación y configuración de sistemas operativos. Administración de usuarios y permisos. Gestión de recursos: Administración de memoria. Administración de procesos. Administración de dispositivos. Seguridad en sistemas operativos: Políticas de seguridad. Mecanismos de autenticación y autorización. Protección contra malware. Copias de seguridad y recuperación de datos. Monitoreo y optimización del rendimiento del sistema.

Programación de Sistemas Operativos. Programación en el espacio del usuario y del kernel. Llamadas al sistema (system calls). Programación de scripts de shell: Shell scripting en Unix/Linux. Comandos y utilidades básicas. Automatización de tareas. Desarrollo de controladores de dispositivos. Programación concurrente: Hilos y sincronización. Exclusión mutua y comunicación entre procesos. Manejo de señales y excepciones. Desarrollo de sistemas de archivos. Prácticas de depuración y manejo de errores.

9 – BASE DE DATOS I

Organización de Datos. Modelos conceptuales (E/R, UML), modelo orientado a objetos, modelo relacional, modelos semiestructurados (XML). Componentes y funciones de un sistema de base de datos. Definición de datos, álgebra relacional. Estructuras de almacenamiento. Modelo Entidad-Relación: Entidad. Relaciones entre entidades. Atributo de las entidades.

Diseño de base de datos. Diseño lógico y diseño físico. Diseño de bases de datos, dependencia funcional, formas normales, descomposición de un esquema, claves primarias y secundarias.

Procesamiento de transacciones, fallas y recuperación, control de concurrencia. Bases de datos distribuidas, problemas que surgen con su explotación.
Fundamentos de Administración y Gestión de Base de Datos. Sistema Gestor de base de datos. Actores y roles del entorno. Recuperación de la información. Gestión de bases de datos. Accesos, permisos y roles. Creación de vistas e índices. Lenguaje SQL/ MySQL y otros. Operaciones: consultas, alta, baja y modificación de registros. Procedimientos almacenados. Disparadores. Usuarios. Transacciones.

10 – PRÁCTICA PROFESIONALIZANTE I

Las Prácticas Profesionalizantes plantean estrategias y actividades formativas que tienen como propósito que los estudiantes consoliden e integren las capacidades o saberes que se corresponden con el perfil profesional en el que se están formando. El primer espacio curricular de práctica profesionalizante pretende iniciar a los estudiantes en el proceso de construcción del rol profesional del Técnico Superior en Desarrollo de Software (TSDS), que se irá proyectando y profundizando durante la carrera. Para cumplir este objetivo, las primeras prácticas estarán referidas a: - Conocer los diferentes contextos de trabajo.
- Identificar diferentes procesos de trabajo, sus características, variables puestas en juego, en ambientes reales de trabajo y/o simulados.
- Reconocer los diferentes actores que conforman el campo profesional.
Todas estas actividades, que se podrán realizar de acuerdo a las posibilidades de articulación institucional con el sector tanto dentro de la institución como fuera de ella, permitirán que los estudiantes tengan una visión más completa e integral sobre el campo profesional, sus características, la diversidad de contextos de intervención, las diferentes relaciones que se ponen en juego, las tensiones y los conflictos que pueden aparecer. También proponen abordar en forma práctica los procesos vinculados a la interacción entre los diversos actores que conforman un equipo de trabajo, identificando los roles y responsabilidades de cada uno y su relación con la tarea profesional del TSDS, profundizando y reflexionando sobre su rol con responsabilidad legal y social.
Este espacio contempla 120 horas que podrán incluir, por un lado, la aproximación del estudiante a experiencias directas y visitas a diversos ámbitos de trabajo con el fin de realizar observaciones, entrevistas, encuestas (métodos de recolección de información) que le permitan conocer las características de los contextos laborales, las vinculaciones con otros actores del sector y/o equipos de trabajo, profundizando y reflexionando sobre las funciones específicas del TSDS. Por otra parte, este espacio también debe comprender horas de trabajo áulico bajo la coordinación del docente, quien podrá implementar diferentes estrategias que le permitan simular todas las etapas de trabajo de creación de software. En este espacio áulico, los estudiantes deberán poner en común e intercambiar con sus compañeros las particularidades de cada simulación realizada, de

cada ámbito relevado, el impacto de los proyectos y de los roles asumidos con el fin de promover el debate y el proceso de aprendizaje colectivo. Para orientar la evaluación, se proponen algunos indicadores que pueden ser utilizados como evidencias, a partir de las cuales se podrá inferir si los estudiantes han alcanzado los objetivos propuestos:

- Comprende el rol profesional del TSDS y sus incumbencias.
- Identifica las características/etapas del proceso de creación de software y elabora los informes correspondientes.
- Reconoce las funciones de los diferentes actores intervinientes en dicho proceso.

SEGUNDO AÑO

11 – MANTENIMIENTO DE INSTALACIONES INFORMÁTICAS

Técnicas de manipulación de equipo electrónico. Herramientas e instrumental de medición y reparación. Técnicas de limpieza y mantenimiento de hardware en CPUs, notebooks, netbooks, AIO, impresoras. Identificación de bloques funcionales. Identificación de averías más comunes en el hardware de CPUs, notebooks, netbooks, AIO e impresoras. Técnicas de armado de CPUs de equipos nuevos. Técnicas de desarme de equipos portátiles. Detección de fallas de hardware con herramientas de software. Reemplazo de componentes fallados. Técnicas de mantenimiento correctivo y preventivo. Elaboración de planes de relevamiento y mantenimiento.

Herramientas de las actividades de instalación y mantenimiento de infraestructura de tecnología de la información. Instrumentos de medición. Teoría de la medición. Teoría de errores de medición.

Instalación, configuración y utilización de plataformas de hardware. Instalación y configuración de sistemas, motores de bases de datos y periféricos.

Mantenimiento, service packs y parches. Actualizaciones y recambios de componentes. IOS, Firmware, actualizaciones. Reemplazo de servidores, migración de datos, software de base. Reducción de riesgos para la seguridad y continuidad de la operación. Administración de periféricos.

Bufferización. Drivers. Administración de memoria. Administración de datos y archivos, problemas de fragmentación de espacios de almacenamiento. Backup. Redundancia de la información, espejo y RAID.

Estructura de directorios. Seguridad y mecanismos de protección. Sistemas operativos multiusuario.

Creación de usuarios o clases de usuarios y asignación de recursos. Configuración y administración de colas de impresión. Intercambio de archivos de datos entre diversas plataformas de hardware.

Clonación de equipos y sistemas. Instalación y configuración de servidor de correo electrónico y

servidor de páginas web y ftp. Procedimientos de registro de incidentes.

12 – HIGIENE Y SEGURIDAD INFORMÁTICA

Normativa vigente en Higiene y Seguridad Laboral asociada a la actividad. Riesgos asociados a la actividad. Técnicas y equipos de seguridad para trabajo en altura. Técnicas y elementos de protección personal para trabajos en Obras en construcción. Técnicas y equipos de protección personal para trabajos con riesgo eléctrico en baja tensión.

Salud y condiciones de trabajo. Concepto de salud, riesgo y accidente. Concepción tradicional de higiene y seguridad en el trabajo. Concepción renovada de CYMAT. Proceso de trabajo. Lay-outs. Mapa de riesgos. Lista de riesgos. Clasificación de riesgos. Riesgos y proceso de trabajo. Enfermedades profesionales. Clasificación de Riesgos. Accidentes. Lesiones. Incapacidad laboral. Ley de Higiene y Seguridad. Ergonomía

13 – MATEMÁTICA APLICADA II

SISTEMAS NUMÉRICOS Y MÉTODOS DE CONTEO. Introducción. Tipos de sistemas numéricos. Conversiones. Operaciones básicas.

INTRODUCCIÓN A LA TEORÍA DE NÚMEROS. divisibilidad. Números primos. Máximo común divisor y mínimo común múltiplo. Algoritmo de la división en los enteros. Algoritmo de Euclides. Primos relativos. Aritmética modular. Relaciones de Congruencia.

ARITMÉTICA MODULAR. Relaciones de Congruencia. Aritmética en (suma, resta, multiplicación, división, elementos inversibles y potencia). Ecuaciones en. Teorema chino de los restos. El pequeño Teorema de Fermat. Expresión matemática de algoritmos de cifrados simétrico, aritmética modular aplicada y curva elíptica. Conformación de claves RSA.

FUNCIONES. Tipos Relaciones; tipos. Conjuntos; Números Reales. Intervalos y entornos. Conjuntos: clasificación. Entorno y entorno reducido. Punto de acumulación. Funciones de variable real. Clasificación. Álgebra de funciones continuas. Composición de funciones. Concepto de límite y funciones. Límites infinitos y al infinito. Continuidad. Cálculo de derivadas. Derivada en un punto. Recta tangente. Función derivada. Determinación de constantes. Aplicación. Cálculo de integrales. Integral definida. Áreas y volúmenes de revolución.

14 – ADMINISTRACIÓN DE SERVIDORES

Roles posibles de un servidor y su injerencia en una red (Proxy, DNS, Terminal Services, Controlador de dominio, etc.). Diferentes tipos de servidores, servidores web, de bases de datos, de aplicaciones y de correo. Sistemas operativos utilizados en la configuración de servidores, como Linux y Windows Server. Instalación y configuración de servidores, gestión de servicios y recursos en un entorno de servidor. Seguridad en la configuración de servidores, políticas de acceso y control, configuración de cortafuegos y medidas de protección. Monitorización y mantenimiento. Herramientas y técnicas para la supervisión del rendimiento y la disponibilidad.

Gestión de copias de seguridad y recuperación ante desastres. Uso de virtualización y contenedores. Eficiencia y escalabilidad de entornos de servidor. Configuración de servidores en la nube, incluyendo la comprensión de plataformas de nube como AWS, Azure y Google Cloud. Realizar configuraciones de nuevos servidores en organizaciones o intervenir en servidores ya instalados en forma remota o local para estudiar su configuración o agregar roles. Seguridad a nivel de protocolo: IP/TCP/UDP, ICMP, HTTP, DNS, DHCP, Correo Electrónico, SSL, Protocolos Wireless, Firewall, Buenas Prácticas. Protocolos y Mecanismos de autenticación: Definición, Vulnerabilidades. Ataques de Acceso, Ataques de reconocimiento, Man in the Middle, Denegación de Servicio. Infraestructura PKI. Certificados. Mecanismos de Seguridad sobre http: XSS, CSRF. Proxy Reverso e Ingress.

15 – INGLÉS TÉCNICO II

Los siguientes descriptores deberán abordarse desde las cuatro macro-habilidades (comprensión lectora y auditiva y producción escrita y oral) y orientarse al campo de desempeño del futuro profesional, desarrollando las competencias básicas fijadas por los estándares del Marco Común Europeo de Referencia para la competencia lingüística de nivel A2: al finalizar el cursado, el estudiante será capaz de comprender frases y expresiones de uso frecuente relacionadas con áreas de experiencia que le son especialmente relevantes (información básica sobre sí mismo y su familia, compras, lugares de interés, ocupaciones, etc). Sabrá comunicarse a la hora de llevar a cabo tareas simples y cotidianas que no requieran más que intercambios sencillos y directos de información sobre cuestiones que le son conocidas o habituales. Podrá describir en términos sencillos aspectos de su pasado y su entorno así como cuestiones relacionadas con sus necesidades inmediatas.

Contenidos mínimos:

El estudiante deberá desarrollar habilidades de producción (habla y escritura) aplicadas a situaciones específicas de la carrera y el año que transita.

Futuro con will. Pasado continuo. Presente perfecto. Presente perfecto continuo. Verbos modales. Condicional 0, 1 y 2. Voz pasiva. Gerundios e infinitivos.

16 – COMUNICACIÓN Y REDES

Definición y concepto de transmisión de datos. Aplicaciones de los sistemas de comunicación de datos. Dispositivos que integran una red. Internet. Organización de Internet. Comunicación de datos a través de una red. Tipos de cableado. Modelo OSI. Modelo TCP/IP. Medios de Networking. Topología de redes LAN. Componentes de una red LAN. Dispositivos Conmutadores. Configuración básica de conmutadores. Redes Virtuales de Área Local (VLAN). Principios básicos de enrutamiento estático y dinámico. Topologías alternativas y optimización de Topología de Redes WAN. Protocolo Punto a Punto. Técnica de comunicación. Seguridad en

redes. Tecnología de red privada virtual (VPN). Servicios de direccionamiento IP. Solución a problemas comunes en redes. SD-Wan. Ruteos. Algoritmo por vector distancia y de estado de enlace. Conceptos de eficiencia en redes. Concepto e implementación de proxies. Descomposición de redes en subredes o grupos de trabajo. Tendido de redes. Cableados. Categorías. Diagnóstico de fallas básicas del enrutador. Herramientas para medir el tráfico y los tiempos de respuesta y retardo. Pruebas de cable. Aplicación práctica del protocolo TCP/IP. Roles funcionales de routers, Access points, Range Extender, CPE, Switches y Controladores de hardware. Conocimiento y configuración de tecnología Wireless: Versiones de WIFI, WDS, WISP. Sistemas MESH. Redes WiFi de grandes áreas. Redes virtuales (VLAN). Simuladores de redes por software.

17 – TALLER DE INSTALACIÓN Y CERTIFICACIÓN DE REDES

Instalación básica de redes. Puesta en marcha. Solución de problemas técnicos y análisis de fallas. Configuración de instalación de dispositivos de red. Equipos inalámbricos. Seguridad de las redes de datos. Resolución de problemas de configuración y puesta en marcha de dispositivos de red. Criterios de mantenimiento de la red. Configuración de Internet y servicios de Internet. Correo electrónico, servidores y servicios. Impresoras de red, colas de impresión. Servidores de páginas web. Servidores FTP, DHCP, DNS. Telnet. Protocolos de autenticación, firmas digitales. Algoritmos de compresión de datos. Capas de seguridad. Instalación y configuración de sistemas operativos para redes. Software del lado del servidor y software cliente. Software para supervisar configuraciones de multiprocesamiento. Máquinas virtuales. Situaciones derivadas de la instalación y administración de redes. Seguridad en centros de cómputos. Protección eléctrica y atmosférica. Mantenimiento preventivo. Informes de contingencia ante situaciones anómalas.

18 – CRIPTOGRAFÍA APLICADA

Criptología clásica: Definición y alcance de la criptología. Objetivos de la criptografía. Introducción a la aritmética modular y algunas definiciones básicas. Historia de la criptografía. Claude Elwood Shannon: Confusión y difusión. Criptografía clásica. Criptoanálisis clásico. Criptología moderna: Criptografía y esteganografía. Principio de Kerckhoffs. Panorama de la Criptología simétrica actual. Panorama de la Criptología asimétrica actual. Integridad, autenticación y no repudio: Control de integridad de la información digital. Concepto y propiedades de funciones Hashing. Funciones Hashing actualmente utilizadas para máxima seguridad. Preservación de evidencias digitales. Autenticación débil y autenticación fuerte. Gestión de Claves. MAC, Firma Digital y Firma Electrónica. Ley de Firma Digital de la República Argentina. Criptosistemas contemporáneos: Cifrados simétricos y asimétricos. Condiciones de los criptosistemas asimétricos. Rivest-Shamir-Adleman (RSA): algoritmo implementado, seguridad del método, encubrimiento de los mensajes. Diffie-Hellman (D-H): algoritmo implementado. Merkle-Hellman (M-H): problema knapsack,

algoritmo de encriptado y desencriptado, seguridad del método. Métodos de ataque conocidos. Autenticación de mensajes & autenticación de transmisores: conceptos y diferencias. Esquemas de Ong-Schnorr-Shamir y Rivest-Shamir-Adleman. Prueba de mínimo conocimiento o de conocimiento cero. Definición de ciberseguridad. Autenticación: Contraseñas, Certificado, Biometría, Tokens, Multifactor. Confidencialidad: criptografía simétrica. Integridad local: Compendios de mensajes, Checksums. Disponibilidad: Copias de Seguridad, Replicación, Clustering. Autorización: Permisos, ACLs, Control de acceso basado en roles, implementaciones en Sistemas de Archivos. No Repudio. Protección de Datos a través de cifrado. Tratamientos de contraseñas. Malware: Tipos, Medios de Propagación, Protección.

19 – AUTOMATIZACIÓN DE SERVICIOS INFORMÁTICOS

Fundamentos de la Automatización: Introducción a los principios de automatización, beneficios en la administración de sistemas y reducción de tareas manuales repetitivas. Scripting y Programación: Uso de lenguajes de scripting (como Bash, PowerShell o Python) para crear scripts que gestionen y optimicen tareas en servidores y redes. Herramientas de Automatización: Familiarización con herramientas de automatización como Ansible, Puppet y Chef, y su uso en la configuración y administración de infraestructura de TI. Automatización de Tareas de Redes y Seguridad: Configuración y monitoreo de dispositivos de red (routers, switches, firewalls) y gestión de políticas de seguridad mediante scripts automatizados. Implementación de Políticas de Seguridad Automatizadas: Uso de herramientas para implementar y monitorear políticas de seguridad, detección de amenazas y respuestas automáticas ante incidentes. Monitoreo y Gestión de Logs: Configuración de sistemas de monitoreo y análisis de logs automatizados para detectar anomalías y mejorar la ciberseguridad. Prácticas de DevOps: Introducción a las prácticas de DevOps aplicadas en la seguridad y automatización de infraestructura. Mantenimiento Automatizado de Sistemas y Redes: Creación de cron jobs y scripts programados para la actualización, parcheo y mantenimiento regular de sistemas y servicios.

20 – ELECTRÓNICA APLICADA

Teoría Atómica. Naturaleza eléctrica de la materia. Partículas fundamentales. Modelo atómico de Bohr. Distribución Discreta y Continua de Cargas. Ley de Coulomb. Campo eléctrico. Principio de superposición. Potencial Eléctrico. Capacidad, Dieléctricos y Energía Electrostática. Energía almacenada en un capacitor. Campo Magnético. Imanes. Polos magnéticos. Movimiento de una carga a través de un campo magnético. Dirección y magnitud de la fuerza magnética. Torque sobre una bobina plana. Fuentes de Campos Magnéticos. Dirección del campo magnético. Campo magnético generado por corriente eléctrica, electroimanes. Principio de funcionamiento de un motor eléctrico. Inducción Magnética. FEM inducida. Ley de Faraday para la FEM inducida. Teoría ondulatoria. Propagación de ondas. Interferencia constructiva y destructiva. Oscilaciones y

resonancia. Espectro Electromagnético. Frecuencias de radio. Luz visible. Propagación en el espacio. Introducción a la Óptica y a la Acústica. Propiedades. Índice de refracción de los materiales. Ley de Snell, aplicación en fibras ópticas. Naturaleza de las ondas sonoras. Efecto Doppler. Fundamento de la teoría de circuitos. Ley de Ohm. Leyes de Kirchoff. Unidades, múltiplos y submúltiplos. Concepto de potencia. Conceptos básicos de corriente continua y corriente alterna.
Fuentes de alimentación. Elementos pasivos. Campo magnético, campo eléctrico, imanes permanentes y electroimanes. Aislación de perturbaciones producidas por campos magnéticos y/o eléctricos. Variación en tiempo y espacio del campo electromagnético.

21 – TECNOLOGÍAS IOT (Internet de la Cosas)

Fundamentos del Internet de las Cosas. Evolución: dispositivos, sensores y actuadores. Plataformas. Protocolos de comunicación: MQTT, CoAP, HTTP y LoRaWAN, arquitectura de redes de sensores interconectados. Plataforma y Herramientas IoT: Arduino, Raspberry Pi y ESP32. Plataformas en la nube para la gestión de IoT (Azure IoT Hub, AWS IoT, Google IoT Core). Integración con APIs y servicios web. Plataforma Arduino. Instalación y configuración del entorno de desarrollo (IDE) de Arduino. Estructura básica de un programa en Arduino. Programación básica: entradas y salidas digitales. Uso de sensores y actuadores con Arduino. Comunicación serial. Manejo de interrupciones y temporizadores. Bloque Proyectos Prácticos con Arduino. Control de LEDs. Lectura de sensores de temperatura y humedad. Control de servomotores. Proyectos Intermedios. Sistemas de alarma con sensores de movimiento. Control de luces y dispositivos a través de relés. Monitoreo y visualización de datos en pantalla LCD. Proyectos Avanzados. Control de robots simples. Domótica: automatización de tareas domésticas. Integración de Arduino con otros dispositivos y plataformas (Bluetooth, Wi-Fi). Seguridad en IoT: desafíos en dispositivos IoT. Técnicas de autenticación, cifrado y control de acceso en entornos IoT. Análisis de vulnerabilidades en dispositivos conectados. IoT en la industria 4.0, agricultura inteligente, salud y ciudades inteligentes. Casos de estudio de implementación de soluciones IoT en diferentes sectores. Despliegue y Mantenimiento de IoT: Monitoreo y gestión remota de dispositivos IoT. Prácticas de mantenimiento y actualizaciones en soluciones IoT.

22 – PRÁCTICA PROFESIONALIZANTE II

La función de asesoramiento para la puesta en marcha de un sistema de tecnologías de la información y comunicación. Roles y actores involucrados. El diagnóstico y la viabilidad de las propuestas. Interpretación de las demandas.
Situaciones derivadas de la instalación y administración de redes. Elementos y criterios de seguridad en centros de cómputos. Protección eléctrica y atmosférica. Mantenimiento preventivo.

Requisitos operativos y condiciones de funcionamiento. Climatización. Puestas a tierra. Manejo de situaciones problemáticas y de emergencias.

Elaboración de un plan de trabajo. Confección de un dossier técnico correspondiente a un proyecto tecnológico y su documentación. Análisis de impacto y de prefactibilidad técnica y económica.

Ejecución del plan de trabajo y su evaluación. Habilidades sociales en la prestación de servicios de tecnologías de la información. El tratamiento de dudas y objeciones. Plan de contingencia.

Instrucciones de procedimiento para planes de contingencia. Para cumplir este objetivo, las prácticas de este espacio estarán referidas a:

- Integrar y contextualizar los saberes desarrollados en la formación, respondiendo a necesidades que implican el desarrollo de productos específicos.
- Desarrollar de manera integral y coordinada en equipos de trabajo los procedimientos propios del desarrollo de software.
- Integrar su tarea dentro del plan de trabajo del equipo de profesionales/colaboradores.

TERCER AÑO

23 – TRATAMIENTO DE INCIDENTES DE CONTINUIDAD DE NEGOCIO

Definición y objetivos del análisis de incidentes, tipos de incidentes de seguridad, normativas y políticas de respuesta, metodologías de análisis, identificación y clasificación de incidentes, recopilación de evidencias, introducción al análisis forense, gestión de incidentes, documentación y reporte, lecciones aprendidas, y estudios de caso. ANÁLISIS DE INTRUSIÓN. File Carving / Data Carving. Metadata de archivos.Trabajando en Browsers y Correos electrónicos.Uso de Nirsoft y Sysinternals Tools. ANÁLISIS DE FALLOS. Recuperación de archivos y particiones eliminadas. Herramientas asociadas. Análisis y recuperación de RAIDS. Análisis y recuperación de discos duros defectuosos.

24 – VIDEOVIGILANCIA Y CONTROL DE ACCESOS

Introducción a los sistemas y normas de video. Tipos de cámaras y entornos de utilización. Lentes y resoluciones en cámaras de CCTV. Sistema de vigilancia analógicos. Configuración de dispositivos DVR (método de grabación, detección movimiento, alertas, visualización en PC y dispositivos móviles). Video vigilancia por dispositivos IP. Configuración de NVR (método de grabación, detección movimiento, alertas, line crossing, lectura de patentes, detección de rostros, integración de dispositivos ONVIF, visualización en PC y dispositivos móviles). Introducción a la telefonía. Introducción a la telefonía IP. Dispositivos de telefonía IP. Dispositivos de interacción con la telefonía analógica. Configuración de Centrales de telefonía IP. Configuración de teléfonos y terminales de telefonía IP.

Tipos de dispositivos de control de acceso y asistencia. Configuración de dispositivos de control de acceso. Configuración de dispositivos de Asistencia. Interacción de dispositivos con cerraduras eléctricas y molinetes. Software de interacción y centralización de dispositivos.Seguridad en el desarrollo de software, identificación de amenazas y vulnerabilidades en aplicaciones. Buenas prácticas en el diseño seguro. Implementación de controles de seguridad a lo largo del ciclo de vida del desarrollo de aplicaciones y técnicas de evaluación - pruebas de penetración y análisis de código fuente - con el objetivo de detectar debilidades antes de la implementación. Gestión de parches y actualizaciones de seguridad en aplicaciones. Mitigación de riesgos. Autenticación y autorización, control de acceso adecuado a los recursos. Encriptación de datos, reposo o tránsito. Protección de información sensible. Educación y concienciación sobre seguridad para desarrolladores. Cultura de seguridad dentro de las organizaciones.

25 – CIBERSEGURIDAD

Fundamentos de la Seguridad Informática. Seguridad física y seguridad lógica. Vocabulario y conceptos básicos. Concepto de incidente, diferencia entre incidente y problema. Confidencialidad en sistemas de cómputos. Vulnerabilidad de los sistemas. Tipos de fallas y ataques a la seguridad.

Estrategias defensivas. Servicios de seguridad: disponibilidad, integridad, confidencialidad, autenticación y no repudio. Técnicas de control de acceso. Privilegios. Autorizaciones. Cifrado de datos. Planes de contingencia. Necesidad de proteger datos y programas, creación, identificación y administración o mantenimiento de archivos de respaldo (backups), así como su recuperación. Software antivirus, antispam, antispyware y contra otro malware, su instalación, actualización y aplicación a nivel corporativo. Parches para actualización de la seguridad de sistemas operativos y demás software de base. Seguridad en lenguajes de programación. Funciones de autenticación e identificación. Firma digital y certificado digital. Aplicaciones seguras. Introducción a la auditoría de software. Logs de eventos relacionados con la autoría y auditoría de procesos.

26 – INGLÉS TÉCNICO III

- **Unidad 1.**

Los siguientes descriptores deberán abordarse desde las cuatro macro-habilidades (comprensión lectora y auditiva y producción escrita y oral) y orientarse al campo de desempeño del futuro profesional, desarrollando las competencias básicas fijadas por los estándares del Marco Común Europeo de Referencia para la competencia lingüística de nivel B1: al finalizar el cursado, el estudiante será capaz de comprender los puntos principales de textos claros y en lengua estándar si tratan sobre cuestiones que le son conocidas, ya sea en situaciones de trabajo, de estudio o de ocio. Sabrá desenvolverse en la mayor parte de las situaciones que pueden surgir durante un viaje por zonas donde se utiliza la lengua. Podrá producir textos sencillos y coherentes sobre temas

que le son familiares o en los que tiene un interés personal. Podrá describir experiencias, acontecimientos, deseos y aspiraciones, así como justificar brevemente sus opiniones o explicar sus planes.

Contenidos mínimos:

El estudiante deberá desarrollar habilidades de producción (habla y escritura) aplicadas a situaciones específicas de la carrera y el año que transita.

Pasado perfecto. Pasado perfecto continuo. Discurso indirecto. Verbos modales en estructuras perfectivas. Condicional 3.

- **Unidad 2.**

Los siguientes descriptores deberán abordarse desde las cuatro macro-habilidades (comprensión lectora y auditiva y producción escrita y oral) y orientarse al campo de desempeño del futuro profesional, desarrollando las competencias básicas fijadas por los estándares del Marco Común Europeo de Referencia para la competencia lingüística de nivel B2: al finalizar el cursado, el estudiante será capaz de entender las ideas principales de textos complejos que traten de temas tanto concretos como abstractos, incluso si son de carácter técnico siempre que estén dentro de su campo de especialización. Podrá relacionarse con hablantes nativos con un grado suficiente de fluidez y naturalidad de modo que la comunicación se realice sin esfuerzo por parte de ninguno de los interlocutores. Podrá producir textos claros y detallados sobre temas diversos así como defender un punto de vista sobre temas generales indicando los pros y los contras de las distintas opciones.

Contenidos mínimos:

El estudiante deberá desarrollar habilidades de producción (habla y escritura) aplicadas a situaciones específicas de la carrera y el año que transita.

Tiempos verbales simples, continuos, perfectos y perfectos continuos contrastados. Verbos modales y expresiones equivalentes, simples y perfectivos. Condicionales 0, 1, 2 y 3. verbos modales en voz pasiva.

27 – LEGISLACIÓN INFORMÁTICA Y ÉTICA PROFESIONAL

Cibercrimen y ciberdelito. Incidencia de la tecnología en la jurisprudencia argentina. Marco legal. ley 26.388 Delitos Informáticos. Amenazas lógicas. Identificación de las amenazas. Ingeniería social, delitos más frecuentes y su tipificación, el código penal argentino. Ley 26.904 Grooming. Ley 27.436 Modificación art. 128 Código Penal (Ciber pornografía). Ley 27.411 Convenio sobre Ciberdelito del Consejo de Europa. (Convención de Budapest). Derechos de autor. Ley 11.723. Régimen legal de la Propiedad Intelectual. Ley 25.326 de Protección de datos personas. Ley 25.891 de Comunicaciones Móviles. Protocolo de Actuación para las Fuerzas de Seguridad en Materia de Ciberdelitos. Principios generales de intervención. Pautas específicas de actuación. Procedimiento. Procedimientos especiales. Embalaje, Transporte y Almacenamiento. Extracción

de la prueba. Cadena de Custodia. Protocolo general de actuación. ISO/IEC 27037. Big Data. Conflictos relacionados con el Big Data. Actividades electrónicas: Internet y las nuevas actividades electrónicas: contratos, e-commerce y propiedad intelectual. Bitcoins. Código QR. El juego online. Cuerpo normativo. Ley 25.922: Ley de promoción de la industria del software. Ley 25.856: El Gobierno Electrónico en la Argentina: TIC en la modernización de la APN. Gobierno Electrónico y legislación. Marco jurídico de la APN. Régimen de contrataciones de la APN. El control interno y la Auditoría. El régimen de Internet.

El campo de la ética. Ciencia, cientificismo y filosofía. El dominio de la ética: el ser y el deber ser. Ética como problemática subjetiva. La reflexión del sujeto libre sobre su accionar. Inviolabilidad, autonomía y dignidad de la persona. Ética y sociedad. La ética como regulación social y compromiso comunitario. Promoción del cambio social. Valores, democracia, desarrollo y burocracia. La ética en el manejo de la información. Desarrollo y uso de las tecnologías de la información. La privacidad y el anonimato. La responsabilidad social de la empresa. La ética en el contexto de las comunicaciones interpersonales: redes sociales. Ética profesional. Código de conducta y ética profesional. La ética en los organismos y organizaciones públicas y privadas. La dimensión ética de las decisiones. Problemáticas éticas del campo profesional. Ética para el profesional de la Ciberseguridad. Definición. Ética como teoría de la moral. Ética y moral como aspectos formativos fundamentales para la privacidad y protección de datos sensibles en redes.

28 – AUDITORÍA DE SEGURIDAD INFORMÁTICA

Tipos de Auditorías: internas, externas, de seguridad, gestión, certificación, acreditación. Objetivos y metodologías. Requerimientos y normativa. Conceptos generales para la elaboración del plan de auditoría. Herramientas para la auditoría de sistemas. Métodos y Técnicas.

Auditoría de infraestructura de TI: evaluación de redes, sistemas operativos y hardware, junto con el análisis de configuraciones y prácticas de mantenimiento. Auditoría de aplicaciones centrada en evaluación de controles de seguridad en el desarrollo de software y la revisión de la gestión de acceso y autenticación. Auditoría de sistemas de gestión, evaluación de sistemas de gestión de seguridad de la información (ISMS) y cumplimiento de políticas internas y externas. Elaboración de informes de auditoría, con claridad y concisión, presentación de hallazgos y recomendaciones.

29 – INVESTIGACIÓN DIGITAL Y CIBERCRIMEN

Fundamentos de Investigación. Cibercrimen y delitos contra la tecnología: investigando ataques web, redes, malware y otros ataques comunes a los equipos tecnológicos, métodos avanzados del cibercrimen. Métodos de ocultamiento, Deep Web, jammers. Cibercrimen y ciberestafas: tipos de estafas que involucran tecnología, phishing, drive by pharming, ransomware, estafas con tarjetas de crédito, rastreo de emails. Cibercrimen y delitos contra las personas: violaciones a la privacidad, grooming, sextorsión, acoso por las redes, revenge porn. Cómo investigar y registrar

legalmente calumnias e injurias a través de las redes. Investigación digital en Internet y Redes Sociales: metodología práctica para la investigación digital de fuentes abiertas en internet, OSINT (Open Source Intelligence). Nociones de Perfilado Criminal del Ciberdelincuente: criminal profiling, tipos de ciberdelincuentes, análisis de comportamiento cibercriminal, modus operandis.

30 – FORENSE DIGITAL

Definición y objetivos de la Ciencia Forense Informática. Pasos del proceso forense informático; identificación, preservación, análisis y presentación, según marco normativo. Protocolo general de actuación. ISO/IEC 27037. Metodología forense para aplicar a pericias de: memorias, discos rígidos, pendrives, logs de seguridad, entre otros. Recursos y herramientas forenses. Uso de distribuciones y herramientas de código abierto. Adquisición de imagen digital forense. Volcado de memoria RAM. Autopsy. Análisis forense de tráfico de red, herramientas para captura y análisis de paquetes e identificación de patrones de tráfico sospechosos. Incidentes en servidores: recolección de evidencia en servidores físicos y virtuales, análisis de registros (logs) y eventos de seguridad. Desafíos de la recolección de evidencia en entornos de nube, identificación de proveedores de servicios en la nube y sus implicaciones forenses. Técnicas de análisis forense en la nube, herramientas y métodos para el análisis de datos en la nube y la recuperación de datos de aplicaciones y servicios. Cibercrimen. Protocolo de Actuación para las Fuerzas de Seguridad en Materia de Ciberdelitos. Principios generales de intervención. Pautas específicas de actuación. Procedimiento. Procedimientos especiales. Embalaje, Transporte y Almacenamiento. Extracción de la prueba. Cadena de Custodia.

31 –ETHICAL HACKING

Ethical Hacking: definición y conducta profesional. Técnicas de ataque físico. Fuerza bruta, técnicas y aplicaciones utilizadas. Vulnerabilidad en sitios WEB. Inyección SQL, técnicas y ejemplos. Ataques password. Ataques Malware. Ataques DOS. Servidores Windows. Servidores Linux. Análisis de casos y errores más comunes. Metodología de pruebas de penetración (pentesting): reconocimiento, escaneo, explotación y reporte. Herramientas y técnicas utilizadas en cada fase. Reconocimiento y recolección de información, técnicas de reconocimiento pasivo y activo. Uso de herramientas para la recolección de datos. OSINT, análisis de vulnerabilidades con herramientas como Nmap y Nessus, explotación de sistemas usando frameworks como Metasploit. Seguridad de aplicaciones web (OWASP Top 10), ataques a redes inalámbricas, escalamiento de privilegios, y pruebas de seguridad en entornos móviles e IoT.

Técnicas para escanear redes y sistemas. Enumeración de servicios y usuarios en sistemas objetivo. Explotación de vulnerabilidades. Post-explotación: técnicas para mantener acceso y escalar privilegios, con la limpieza de huellas para mitigar la detección. Pruebas de penetración, diseño y ejecución, con énfasis en la elaboración de informes claros sobre los resultados.

32 – PRÁCTICA PROFESIONALIZANTE III

En el último espacio de Práctica Profesionalizante, los estudiantes deberán elaborar un proyecto de carácter integrador que contemple todos los aprendizajes adquiridos previamente y su transferencia a un recorte concreto de la realidad. El objetivo principal de este trabajo es proponer alternativas tecnológicas que optimicen y/o innoven en relación a problemáticas sociales y/o específicas de su profesión, desarrollando e implementando sistemas web, móviles u otro tipo de acuerdo a requerimientos de usuarios.

Por su carácter integral, estas prácticas profesionalizantes requieren poner en juego diversas actividades propias del quehacer profesional. Para ello los estudiantes, en forma grupal o individual, irán tomando una serie de decisiones y realizando un conjunto de actividades que les permita llegar al objetivo final.

Este espacio curricular está organizado por un taller grupal y el trabajo en campo. En el taller, los estudiantes preparan su salida al campo, ponen en común sus vivencias y realizan la síntesis y conclusiones de las experiencias. El trabajo en campo corresponderá a la inserción de los estudiantes en el contexto laboral o en aquel que mejor se aproxime a las condiciones reales. La estrategia de evaluación final consistirá en la presentación y defensa del proyecto.

En la planificación de esta unidad curricular, deberán preverse un número suficiente de encuentros presenciales para desarrollar los requisitos y criterios que deberán tener en cuenta los estudiantes para la elaboración del proyecto, a través de materiales y guías de trabajo. En las clases presenciales los estudiantes planifican su trabajo y consultan dudas frente a la elaboración del proyecto. Se socializan las experiencias que van adquiriendo, se gestionan los permisos y seguros que se requieran para realizar visitas en contextos de trabajo, el uso del laboratorio de programación para la elaboración del trabajo. El objetivo principal de los encuentros será la reflexión grupal sobre las dudas y los avances con el fin de lograr un ámbito de aprendizaje colaborativo.

El futuro Técnico Superior deberá elaborar un Proyecto Final que sea coherente con el cúmulo de conocimientos adquiridos durante toda la carrera, demostrando su capacidad de crear un proyecto tecnológico acorde con las nuevas tecnologías y factible de ser implementado en el mundo real:

- Definir la temática disparadora del proyecto final de carrera.
- Integrar los conocimientos adquiridos durante la carrera
- Elaborar un plan de trabajo adecuado al proyecto final.
- Realizar exposiciones orales breves que le permita hacer la defensa final del proyecto.
- Honestidad intelectual. Responsabilidad ético - legal y social.
- Manejo adecuado del vocabulario científico y técnico de su campo laboral

El desarrollo del Proyecto Integrador comprende una serie de encuentros grupales presenciales en los cuales los estudiantes planifican su trabajo, socializan las experiencias que van adquiriendo

en cada una de las etapas de los diversos proyectos y elaboran conclusiones que permitan aprendizajes colectivos.

El docente y las autoridades de la institución educativa acordarán los ámbitos destinados a la realización de las prácticas externas de los estudiantes para el desarrollo del proyecto. Los contextos deberán ser diversos y pertinentes en relación a los objetivos planteados, incluyendo todos los requerimientos para que las actividades prácticas se realicen en contextos seguros.

Prácticas profesionalizantes: Es un espacio de realización de actividades ligadas al campo real de trabajo que tienen como propósito la aproximación progresiva a las múltiples tareas que constituyen el desempeño profesional, a partir de actividades de reflexión y acción. Su desarrollo debe ser progresivo a lo largo de toda la carrera y debe contemplar el análisis permanente de la experiencia que se desarrolla en el contexto de trabajo a través, por ejemplo, de talleres de análisis y reflexión paralelos al desarrollo de la práctica externa, cuya principal finalidad es facilitar procesos que promuevan en los estudiantes un desempeño profesional idóneo y éticamente orientado. Si bien las prácticas profesionalizantes pueden asumir diferentes formatos, sintéticamente pueden reducirse a dos: a) pasantías, prácticas en ambientes de trabajo y/ o formación en ambientes productivos (reales y/o simulados), b) proyectos orientados a la resolución de problemáticas y necesidades a nivel institucional/organizacional, local y/ o regional. En todos los casos, las prácticas profesionalizantes son organizadas y coordinadas por la institución educativa a través de los entornos formativos existentes y los acuerdos que se generen para la realización por fuera de ella. Cualquiera sea el formato adoptado, los IES tienen la responsabilidad de planificar, organizar, supervisar y evaluar las prácticas profesionalizantes. La planificación y desarrollo de esta unidad curricular deberá asegurar, de manera continua a lo largo de cada cuatrimestre, instancias presenciales a cargo del equipo docente, las cuales tendrán como actividad específica la realización del seguimiento de las distintas actividades que las/os estudiantes deberán efectuar en función de las características de cada una de las prácticas profesionalizantes establecidas en el diseño curricular.

5. RÉGIMEN DE REGULARIDAD, PROMOCIÓN, EVALUACIÓN Y ACREDITACIÓN. Cfr. RESOLUCIÓN RAM VIGENTE.

Cfr. RESOLUCIÓN 1286-DGE-2024 RAM, RAI y demás normativas vigentes

5.1. Espacios Curriculares acreditables por formación previa

Las acreditaciones se realizarán cuando haya certificación de organismos oficiales (DGE, Min. de Educación, Min de Trabajo, entre otros) o por evaluación de idoneidad a cargo del Instituto de Educación Superior, junto con el sector socio – productivo correspondiente

5.2. Espacios curriculares de acreditación directa

Se regirán por el sistema de acreditación directa, según lo dispone el Artículo 46 inciso "a" del apartado referido a las trayectorias estudiantiles correspondiente al Reglamento Académico Marco (Res. N° 1286-DGE-2024), los siguientes espacios curriculares:

6. RÉGIMEN DE CORRELATIVIDADES*

ESPACIO CURRICULAR	REGULAR PARA CURSAR	APROBADA PARA ACREDITAR
PRIMER AÑO		
10 – PRÁCTICA PROFESIONALIZANTE I	-----	PROGRAMACIÓN I BASE DE DATOS I
SEGUNDO AÑO		
11 – SOPORTE DE INSTALACIONES INFORMÁTICAS	ARQUITECTURA DE DISPOSITIVOS PRÁCTICA PROFESIONALIZANTE I	PRÁCTICA PROFESIONALIZANTE I
12 – HIGIENE Y SEGURIDAD INFORMÁTICA	-----	-----
13 – MATEMÁTICA APLICADA II	MATEMÁTICA APLICADA	MATEMÁTICA APLICADA
14 – ADMINISTRACIÓN DE SERVIDORES	ARQUITECTURA DE DISPOSITIVOS	ARQUITECTURA DE DISPOSITIVOS
15 – INGLÉS TÉCNICO II	INGLÉS TÉCNICO I	INGLÉS TÉCNICO I
16 – COMUNICACIÓN Y REDES	BASE DE DATOS I	BASE DE DATOS I
17 – TALLER DE INSTALACIÓN Y CERTIFICACIÓN DE REDES	ARQUITECTURA DE DISPOSITIVOS	ARQUITECTURA DE DISPOSITIVOS
18 – CRIPTOGRAFÍA APLICADA	MATEMÁTICA APLICADA	MATEMÁTICA APLICADA
19 – AUTOMATIZACIÓN DE SERVICIOS INFORMÁTICOS	-----	-----
20 – ELECTRÓNICA APLICADA	-----	-----
21 – TECNOLOGÍAS IOT	-----	ELECTRÓNICA APLICADA
22 – PRÁCTICA PROFESIONALIZANTE II	PRÁCTICA PROFESIONALIZANTE I	PRÁCTICA PROFESIONALIZANTE I
TERCER AÑO		
23 – TRATAMIENTO DE INCIDENTES DE CONTINUIDAD DE NEGOCIO	HIGIENE Y SEGURIDAD INFORMÁTICA	HIGIENE Y SEGURIDAD INFORMÁTICA
24 – VIDEOVIGILANCIA Y CONTROL DE ACCESOS	TECNOLOGÍAS IOT	TECNOLOGÍAS IOT

25 – CIBERSEGURIDAD	-----	AUTOMATIZACIÓN DE SERVICIOS INFORMÁTICOS
26 – INGLÉS TÉCNICO III	INGLÉS TÉCNICO II	INGLÉS TÉCNICO II
27 – LEGISLACIÓN INFORMÁTICA Y ÉTICA PROFESIONAL	-----	-----
28 – AUDITORÍA DE SEGURIDAD INFORMÁTICA	-----	LEGISLACIÓN INFORMÁTICA Y ÉTICA PROFESIONAL
29 – INVESTIGACIÓN DIGITAL Y CIBERCRIMEN	-----	-----
30 – FORENSE DIGITAL	-----	INVESTIGACIÓN DIGITAL Y CIBERCRIMEN
31 – ETHICAL HACKING	-----	LEGISLACIÓN INFORMÁTICA Y ÉTICA PROFESIONAL INVESTIGACIÓN DIGITAL Y CIBERCRIMEN
32 – PRÁCTICAS PROFESIONALIZANTES III	PRÁCTICA PROFESIONALIZANTE II	PRÁCTICA PROFESIONALIZANTE II

***Para poder cursar tercer año el estudiante deberá tener acreditado todos los espacios curriculares de primer año y la mitad más uno de los espacios curriculares de segundo año.**

RÉGIMEN DE ASISTENCIA

Cfr. RESOLUCIÓN 1286-DGE-2024 RAM, RAI y demás normativas vigentes

IMPLEMENTACIÓN DE LA CARRERA

1. Recursos

1.1. Humanos

Se seleccionarán aquellos docentes que cumplimenten los requisitos previstos en la normativa específica sobre el ingreso y/o reasignación de docentes correspondiente al Nivel Superior jurisdiccional (Decreto Ley Nº 530/18 – Cap. III) y la Ley de Educación Provincial N° 6970 Título V- De la Educación Superior, Capítulo IV- Gobierno de la Educación Superior no Universitaria, Art. 112º, inc. c)

PERFILES DOCENTES NECESARIOS PARA CUBRIR LOS ESPACIOS CURRICULARES:

El perfil profesional docente establecido para cada espacio curricular debe ser considerado prioritario al momento de asignar las horas de este. Se priorizará a los postulantes con formación docente acreditable, con conocimiento, posgrado, antecedentes y experiencia en el

campo (Decreto 530-DGE- 2018). En los espacios curriculares de práctica profesionalizante, la experiencia laboral en el campo de formación es excluyente. Los espacios con sus perfiles docentes correspondientes son los siguientes.

ESPACIO CURRICULAR	PERFIL PROFESIONAL
1 – PROGRAMACIÓN I	Licenciado en Informática, Ingeniero en Sistemas/ Informática/ Computación.
2 – MATEMÁTICA APLICADA	Licenciado /Profesor de Matemática. Ingeniero en sistemas de información.
3 – LÓGICA COMPUTACIONAL	Profesor y/o licenciado en Matemática. Licenciado y/o ingeniero en Sistemas/ Informática/ Computación
4 – INGLÉS TÉCNICO I	Profesor/Licenciado en Inglés
5 – ALFABETIZACIÓN ACADÉMICA	Licenciado / Prof. en Lengua y Literatura. Licenciado /Profesor en Comunicación Social.
6 – SEMINARIO NUEVAS TECNOLOGÍAS	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
7 – ARQUITECTURA DE DISPOSITIVOS	Licenciado en Informática, Ingeniero en Sistemas/ Informática/ Computación.
8 – SISTEMAS OPERATIVOS I	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
9 – BASE DE DATOS I	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
10 – PRÁCTICA PROFESIONALIZANTE I	Licenciado y/o Ingeniero en Sistemas/Informática/ Computación con formación **y** experiencia pedagógica.
11 – MANTENIMIENTO DE INSTALACIONES INFORMÁTICAS	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
12 – HIGIENE Y SEGURIDAD INFORMÁTICA	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
13 – MATEMÁTICA APLICADA II	Licenciado /Profesor de Matemática. Ingeniero en sistemas de información.
14 – ADMINISTRACIÓN DE SERVIDORES	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
15 – INGLÉS TÉCNICO II	Profesor/Licenciado en Inglés
16 – COMUNICACIÓN Y REDES	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.

17 – TALLER DE INSTALACIÓN Y CERTIFICACIÓN DE REDES	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
18 – CRIPTOGRAFÍA APLICADA	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
19 – AUTOMATIZACIÓN DE SERVICIOS INFORMÁTICOS	Licenciado y/o Ingeniero en Sistemas/Informática/ Computación con formación y experiencia pedagógica
20 – ELECTRÓNICA APLICADA	Ingeniero en Electrónica. Ingeniero en Electromecánica. Ingeniero en computación
21 – TECNOLOGÍA IOT	Ingeniero en Electrónica. Ingeniero en Electromecánica. Ingeniero en computación
22 – PRÁCTICA PROFESIONALIZANTE II	Licenciado y/o Ingeniero en Sistemas/Informática/ Computación con formación y experiencia pedagógica
23 – TRATAMIENTO DE INCIDENTES DE CONTINUIDAD DE NEGOCIO	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
24 – VIDEOVIGILANCIA Y CONTROL DE ACCESOS	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
25 – CIBERSEGURIDAD	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación
26 – INGLÉS TÉCNICO III	Profesor/Licenciado en Inglés
27 – LEGISLACIÓN INFORMÁTICA Y ÉTICA PROFESIONAL	Profesor/ Licenciado en Ciencias Jurídicas y Contables. Abogado
28 – AUDITORÍA DE SEGURIDAD INFORMÁTICA	Licenciado y/o Ingeniero en Sistemas/Informática/ Computación con formación **y** experiencia pedagógica
29 – INVESTIGACIÓN DIGITAL Y CIBERCRIMEN	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
30 – FORENSE DIGITAL	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
31 – ETHICAL HACKING	Licenciado y/o Ingeniero en Sistemas/ Informática/ Computación.
32 – PRÁCTICAS PROFESIONALIZANTES III	Licenciado y/o Ingeniero en Sistemas/Informática/ Computación con formación **y** experiencia pedagógica

Entorno Formativo en el lugar dónde se dictará la propuesta formativa.

- **Condiciones edilicias**

Edificios propios del IES o en edificios compartidos con otras entidades de educación oficial o

privada.

- **Equipamientos**

Proyectores multimedia, Equipos de informática portátiles, Herramientas de uso cotidiano. Elementos didácticos para la enseñanza de materias relacionadas con la informática *(Hardware diverso, elementos activos de red, Instaladores de software, etc.)*

Medios accesibles para traslado para la práctica en el campo laboral

- **Instalaciones**

Aulas, Salas de Informática, Servicios de Internet

- **Ámbitos de prácticas**

Cfr. Resolución N° 2992-DES-15 “Acuerdo Marco de Prácticas Profesionalizantes” Reglamentos Institucionales de Prácticas Profesionalizantes. Aulas, Laboratorios propios, convenios con empresas. Cobertura de seguro para docentes y estudiantes en salidas de campo.

- **Bibliotecas técnicas especializadas**

Bibliotecas propias. Biblioteca específica de la carrera. Bibliotecas virtuales. Indispensable el acceso a Internet.

CURSO DE INGRESO

Cfr. RESOLUCIÓN N° 1286- DGE-2024 (RAM) y RAI vigentes.

Se sugiere implementar en los cursos nivelatorio de ingreso el dictado de contenidos de **Lógica e Introducción a la Programación.**