DIPLOMATURA EN CIBERSEGURIDAD

1. IDENTIFICACIÓN DE LA PROPUESTA

Denominación: Diplomatura en Ciberseguridad
Tipo de certificación: Diplomatura
Nivel: Formación continua / educación no formal articulable con pregrado
Comienzo: 4 de agosto de 2026

Duración: 1 (un) año – 2 cuatrimestres
Modalidad: A distancia con clases sincrónicas online, 2 clases por semana (martes y jueves de 18:30 a 21:30hs.)
Carga horaria total: 216 horas
Créditos académicos (SACAU): 7.2 créditos
Unidad Académica: FUNDETEC – (futuro Instituto Tecnológico Monserrat – ITM)
Área disciplinar: Ciencias de la Información, Informática y Telecomunicaciones

---

2. FUNDAMENTACIÓN

El crecimiento sostenido de la digitalización en los sectores productivos, gubernamentales y sociales ha incrementado significativamente la exposición a riesgos cibernéticos, generando una demanda concreta de recursos humanos con formación específica en seguridad de la información.

La Ciberseguridad constituye un campo interdisciplinario que integra conocimientos técnicos, normativos y organizacionales, requiriendo perfiles capaces de comprender tanto las tecnologías como los riesgos asociados a su uso.

La presente Diplomatura en Ciberseguridad se orienta a brindar una formación inicial intensiva, con fuerte énfasis en la aplicación práctica, alineada con estándares internacionales (ISO 27000, NIST), y diseñada estratégicamente como trayecto formativo articulable con la **Tecnicatura Universitaria en Ciberseguridad**, permitiendo el reconocimiento de equivalencias parciales en futuras trayectorias académicas.

---

3. OBJETIVOS

3.1 Objetivo General

Formar recursos humanos con competencias iniciales en ciberseguridad, capaces de colaborar en la implementación, operación y mejora de controles de seguridad informática en entornos organizacionales.

3.2 Objetivos Específicos

- Introducir los fundamentos de la seguridad de la información
- Desarrollar capacidades básicas en sistemas operativos, redes y programación
- Aplicar herramientas de detección y mitigación de amenazas
- Comprender marcos normativos y regulatorios
- Incorporar nociones de gestión de riesgos e incidentes
- Desarrollar habilidades de comunicación técnica

---

4. PERFIL DEL EGRESADO

El egresado será capaz de:

- Comprender los principios fundamentales de la seguridad de la información
- Identificar vulnerabilidades básicas en sistemas, redes y aplicaciones
- Colaborar en la implementación de controles de seguridad
- Participar en procesos iniciales de gestión de incidentes
- Interpretar estándares y marcos normativos
- Elaborar reportes técnicos y documentación profesional

---

5. ALCANCES DE LA CERTIFICACIÓN

El Diplomado podrá:

- Integrar equipos técnicos en áreas de ciberseguridad
- Colaborar en tareas de monitoreo y soporte de seguridad
- Asistir en la implementación de controles básicos
- Participar en análisis preliminar de vulnerabilidades
- Elaborar documentación técnica

---

6. REQUISITOS DE INGRESO

- Título de nivel secundario completo
- Conocimientos básicos de informática (no excluyente)

---

7. ORGANIZACIÓN CURRICULAR

La Diplomatura se organiza en **dos cuatrimestres**, estructurada en módulos autocontenidos, sin correlatividades obligatorias, permitiendo trayectorias flexibles.

PRIMER CUATRIMESTRE

Código	Asignatura	Régimen	Hs.	Créditos
DCS01	Introducción a la Ciberseguridad	Cuatrimestral	21	0.7
DCS02	Sistemas Operativos y Entornos Seguros	Cuatrimestral	21	0.7
DCS03	Redes y Fundamentos de Seguridad	Cuatrimestral	24	0.8
DCS04	Programación Aplicada a la Seguridad	Cuatrimestral	21	0.7
DCS05	Comunicación Técnica	Cuatrimestral	21	0.7

Subtotal: 108 horas – 3.6 créditos

SEGUNDO CUATRIMESTRE

Código	Asignatura	Régimen	Hs.	Créditos
DCS06	Normas y Estándares de Seguridad	Cuatrimestral	18	0.6
DCS07	Seguridad en Redes	Cuatrimestral	18	0.6
DCS08	Análisis de Riesgos e Incidentes	Cuatrimestral	18	0.6
DCS09	Hacking Ético	Cuatrimestral	18	0.6
DCS10	Legislación y Cibercrimen	Cuatrimestral	18	0.6
DCS11	Auditoría e Informática Forense / Clave Pública y Firma Digital	Cuatrimestral	18	0.6

Subtotal: 108 horas – 3.6 créditos

TOTAL GENERAL

216 horas – 7.2 créditos SACAU

---

8. CONTENIDOS MÍNIMOS

(Se mantienen en formato ITM, ya alineados con la Tecnicatura)

Introducción a la Ciberseguridad

Concepto de seguridad de la información. Principios de confidencialidad, integridad y disponibilidad. Amenazas, vulnerabilidades y riesgos. Superficie de ataque y modelos básicos de amenazas. Tipos de ataques informáticos. Seguridad lógica y física. Gestión

inicial de incidentes. Introducción a marcos normativos internacionales. Principios éticos de la ciberseguridad y responsabilidad profesional.

Sistemas Operativos y Entornos Seguros

Gestión de usuarios, grupos y permisos. Configuración segura de sistemas operativos. Hardening de entornos Windows y Linux. Registro y monitoreo de eventos. Control de acceso y políticas de seguridad. Administración segura de servidores. Gestión de parches y actualizaciones. Protección contra malware a nivel sistema.

Redes y Fundamentos de Seguridad

Redes: Sistemas de detección y prevención de intrusiones. Redes Privadas Virtuales (VPN). Segmentación avanzada y control de tráfico. Protocolos seguros. Monitoreo de tráfico y análisis básico de eventos. Arquitecturas seguras de red y enfoque de defensa en profundidad.

Bases de Datos: Modelos de bases de datos. Lenguaje SQL y consultas estructuradas. Administración de bases de datos relacionales. Gestión de usuarios, roles y privilegios. Seguridad en bases de datos. Protección de información sensible. Copias de seguridad, recuperación de datos y auditoría de accesos.

Aplicaciones: Ciclo de vida del desarrollo de software. Principios de programación segura. Desarrollo web seguro. Manejo seguro de sesiones. Integración segura con bases de datos. Introducción a pruebas de seguridad y control de vulnerabilidades.

Programación aplicada a la Seguridad

Algoritmos y estructuras de control. Programación estructurada y orientada a objetos. Manejo de archivos. Depuración de código. Principios de programación segura. Validación y sanitización de entradas. Introducción a vulnerabilidades comunes. Desarrollo de scripts para automatización de tareas básicas de seguridad.

Comunicación Técnica

Comunicación oral y escrita en entornos técnicos. Redacción de informes técnicos y reportes de incidentes. Presentaciones profesionales. Comunicación organizacional. Trabajo colaborativo. Técnicas básicas de negociación. Comunicación en contextos de crisis tecnológica.

Normas y Estándares de Seguridad

Gobernanza de la seguridad de la información. Normas ISO 27001 y familia ISO 27000. ISO 27002 (controles) e introducción a ISO 27005 (riesgos). Marco NIST Cybersecurity Framework. Políticas y procedimientos de seguridad. Auditorías de cumplimiento y control documental.

Seguridad en Redes

Diseño seguro de redes. Arquitectura tradicional y moderna. LAN, WAN y flujos. Zonas de seguridad. Segmentación y VLANs. Enrutamiento seguro. Defensa en capas. DMZ y servicios expuestos. Zero Trust y control lateral. Gestión de accesos. Contingencia (backups, snapshots).

Alta disponibilidad y replicación de la infraestructura. Segmentación de redes. Gestión de permisos y autenticación de red (PROXY, RADIUS). Configuración segura de equipos de red. Conexiones seguras (VPN, SSH, etc). Protocolos seguros (SSL, TLS, etc). Seguridad WIFI

Concepto de Firewall. Tipos de firewall. Firewall de red y host. Firewalls con IPS y IDS. Filtrado de tráfico. Control de acceso. Reglas de seguridad. Estado de conexiones. NAT y puertos. DMZ aplicada. Configuración pfSense. Logs y monitoreo.

Análisis de Riesgos e Incidentes

Fundamentos de gestión del riesgo en seguridad informática. Metodologías de análisis de riesgos (enfoque ISO 27005 – nivel introductorio). Evaluación de vulnerabilidades. Matrices de riesgo. Planes de contingencia. Gestión de incidentes y respuesta inicial. Continuidad operativa y planes básicos de recuperación ante desastres.

Hacking ético

Metodologías estructuradas de pruebas de penetración. Fases del pentesting: reconocimiento, análisis, explotación controlada y reporte. Herramientas de evaluación de vulnerabilidades. Elaboración de informes técnicos y ejecutivos con recomendaciones.

Legislación y Cibercrimen

Legislación: Marco legal argentino en delitos informáticos. Protección de datos personales. Evidencia digital y principios básicos de cadena de custodia. Responsabilidad profesional. Normativas internacionales de referencia. Dimensión ética en el tratamiento de información sensible.

Cibercrimen: Tipologías del cibercrimen. Modalidades delictivas digitales. Técnicas básicas de investigación digital. Cooperación internacional en materia de ciberdelito. Prevención organizacional del delito informático. Rol de organismos de seguridad.

Auditoría e Informática Forense / Clave Pública y Firma Digital

Auditoría e Informática Forense: Metodologías básicas de auditoría informática. Recolección y preservación de evidencia digital. Principios de cadena de custodia. Análisis forense inicial en dispositivos y registros. Herramientas básicas de análisis digital. Elaboración de informes técnicos

Clave Pública y Firma Digital: Fundamentos de criptografía simétrica y asimétrica. Infraestructura de clave pública). Certificados digitales y autoridades certificantes. Protocolos criptográficos. Firma digital conforme normativa vigente. Autenticación y gestión básica de identidades digitales.

---

9. ARTICULACIÓN CON CARRERAS DE PREGRADO

La presente Diplomatura podrá ser reconocida como trayecto formativo equivalente parcial dentro de carreras de pregrado afines, en particular la:

➞ Tecnicatura Universitaria en Ciberseguridad del futuro ITM

Asignaturas potencialmente equivalentes:

- Introducción a la Ciberseguridad
- Computación y Sistemas Operativos
- Redes de Computadoras
- Comunicación Profesional
- Normas y Estándares
- Legislación en Ciberseguridad
- Programación (parcial)
- Análisis de Riesgos (parcial)

---

10. METODOLOGÍA DE ENSEÑANZA

- Clases virtuales sincrónicas online
- Resolución de casos reales en clase
- Apuntes elaborados por los docentes
- Bibliografía de referencia

---

11. EVALUACIÓN

- Trabajo Final Individual por módulo

---

12. CERTIFICACIÓN

Quienes hubiesen aprobado todos los Trabajos Finales de los módulos y cumplido con el 75% de asistencia a las clases se les otorgará el Certificado de:

🎓 **“Diplomado/a en Ciberseguridad” – FUNDETEC**

---

13. OBSERVACIÓN NORMATIVA

La presente propuesta se enmarca en la formación continua, pudiendo ser integrada a trayectos académicos formales conforme normativa vigente y criterios institucionales de reconocimiento de equivalencias.

---

14. INSCRIPCIONES Y CONSULTAS

Para inscribirse y realizar consultas enviar un mail a inscripciones@fundetec.org.ar

---