Fundamentos Prácticos de Ciberseguridad

Desarrollado por la **Escuela de Seguridad Privada** — el curso que transforma a cualquier persona en un defensor activo de la infraestructura digital.

Inscríbete Ahora | Ver Programa Completo

¿De Qué Trata Este Curso?

En la era digital moderna, la información se ha transformado en el activo más valioso tanto a nivel personal como empresarial. Frente al incremento exponencial de las amenazas digitales, entender cómo proteger nuestros sistemas, redes y datos ya no es opcional: es una **primera línea de defensa fundamental**.

El curso está diseñado de forma intencional y progresiva para guiar a los participantes desde los conceptos más básicos de la seguridad digital hasta las operaciones de seguridad avanzadas. A través de un enfoque sumamente didáctico, con actividades prácticas y análisis de situaciones reales, los alumnos desarrollarán habilidades clave para convertirse en defensores activos de la infraestructura digital.

¿A Quién Va Dirigido?

Absolutamente a cualquier persona: profesionales de la seguridad o colaboradores de cualquier área organizacional. **No se requiere experiencia previa en tecnología.**

Metodología

Aprendizaje progresivo dividido en **5 grandes módulos** estructurados de manera secuencial. Cada módulo construye sobre el anterior para asegurar una comprensión sólida y duradera.

Estructura del Curso: 5 Módulos Esenciales

El plan de estudios está minuciosamente organizado para cubrir de manera integral los pilares técnicos, normativos y humanos de la ciberseguridad. Cada módulo aborda una dimensión crítica de la protección digital.

1	**Fundamentos y Factor Humano** Introducción a la Tríada CIA (Confidencialidad, Integridad y Disponibilidad) y tácticas de Ingeniería Social. El eslabón más vulnerable: las personas.
2	**Arquitectura de Redes Seguras** Modelo OSI de 7 capas, defensa en profundidad, Firewalls, switches, routers, zonas DMZ y redes privadas virtuales (VPN).
3	**Ecosistema del Malware** Tipos de software malicioso (Virus, Gusanos, Troyanos, Ransomware, Botnets, Fileless Malware) y las 7 fases del modelo Cyber Kill Chain.
4	**Identidad y Criptografía** Cifrado Simétrico vs. Asimétrico, Firmas Digitales, Arquitectura IAM, Autenticación Multifactor (MFA) y Principio de Menor Privilegio.
5	**Operaciones, Ética y Cumplimiento** Centros SOC, sistemas SIEM, ciclo NIST de respuesta a incidentes, hacking ético y marcos legales (RGPD, Ley 21.663 y Ley 21.719 de Chile).

¿Qué Aprenderás al Finalizar el Curso?

Al completar este proceso formativo, el alumno habrá transformado su perspectiva digital y será completamente capaz de aplicar conocimientos de ciberseguridad en entornos personales y laborales. Estos son los objetivos de aprendizaje concretos que alcanzarás:

Garantizar los Pilares de la Información

Aplicar activamente los principios de confidencialidad, integridad y disponibilidad (Tríada CIA) en tus entornos personales y laborales.

Mapear la Comunicación de Datos

Dominar conceptualmente el Modelo OSI de 7 capas para saber exactamente en qué nivel aplicar un control técnico específico de seguridad.

Implementar Escudos Criptográficos y de Identidad

Utilizar herramientas profesionales como gestores de contraseñas seguros, aplicaciones de MFA y soluciones de cifrado de archivos en el día a día.

Reconocer y Neutralizar la Ingeniería Social

Identificar de forma temprana correos, mensajes o llamadas fraudulentas (phishing, pretexting y baiting), adoptando una mentalidad proactiva y preventiva.

Categorizar y Detectar Infecciones

Distinguir los diferentes tipos de malware y diagnosticar si un dispositivo está comprometido mediante señales de alerta: lentitud, archivos cifrados, comportamientos inusuales.

Responder Según Estándares y la Ley

Ejecutar las fases NIST de respuesta a incidentes (desde la preparación hasta las lecciones aprendidas) bajo una conducta ética y alineada a las regulaciones locales como la ANCI y el CSIRT Nacional en Chile.

Conceptos Clave que Todo Alumno Debe Dominar

Para asegurar el éxito del estudiante, el curso destaca la asimilación de los siguientes conceptos críticos e indispensables que forman la columna vertebral de cualquier estrategia de ciberseguridad moderna.

🔒 La Tríada CIA

El cimiento de cualquier política de seguridad: **Confidencialidad** (datos legibles solo por personal autorizado), **Integridad** (datos exactos y sin alteraciones) y **Disponibilidad** (datos listos cuando se necesiten).

💀 Ransomware: El Secuestro Digital

Una de las amenazas más costosas a nivel mundial. El curso enseña la relevancia crítica de las copias de seguridad fuera de línea (backups) como única defensa real ante el cifrado malicioso de datos.

🛡️ Defensa en Profundidad

Ninguna solución mágica es suficiente de forma aislada. Es vital estructurar **múltiples barreras** tecnológicas, físicas y administrativas concurrentes para una protección real.

🔑 Criptografía Híbrida

Los sistemas modernos fusionan la **velocidad del cifrado simétrico** con la **seguridad de distribución de claves del cifrado asimétrico** para proteger la información en tránsito y en reposo.

⏱️ El Reloj de las 3 Horas

Bajo la Ley 21.663 de Chile, las organizaciones de importancia vital están obligadas por ley a reportar incidentes graves al CSIRT Nacional en un plazo máximo de 3 horas. La ciberseguridad es un requerimiento legal ineludible.

Operaciones de Seguridad, Ética y Cumplimiento

Saber cómo responder ante incidentes, actuar con ética y cumplir con las normativas es tan importante como conocer las amenazas técnicas. Proteger datos, mantener la confianza y evitar consecuencias legales son los tres pilares de este bloque final, el más operativo y aplicado de todo el programa.

Este módulo se divide en tres grandes pilares operacionales: el **Ciclo de Respuesta a Incidentes bajo el Marco NIST**, la **Ética Profesional en Ciberseguridad** y el **Cumplimiento Normativo y Marcos Legales** vigentes tanto a nivel internacional como en Chile específicamente.

El Ciclo de Respuesta a Incidentes: Marco NIST

Proceso estructurado y no lineal para reaccionar de forma rápida y eficaz ante amenazas, minimizando daños y restaurando operaciones. Consta de **6 fases críticas** donde cada decisión debe documentarse manteniendo comunicación constante entre equipos.

Preparación | **Detección** | **Contención** | **Erradicación** | **Recuperación**

Cada fase tiene ejemplos prácticos aplicados al contexto de la seguridad privada: desde simulacros trimestrales de ransomware en la **Fase 1**, hasta la convocatoria de reuniones post-incidente para actualizar manuales de procedimientos en la **Fase 6**. La acción clave transversal es siempre documentar, aislar sin destruir evidencia y verificar exhaustivamente antes de declarar el incidente cerrado.

Ética Profesional en Ciberseguridad

La ética profesional es el conjunto de principios y normas que guían el comportamiento responsable de los especialistas en ciberseguridad. Estos deben actuar con **integridad, honestidad, responsabilidad y transparencia**, evitando el uso indebido de sus conocimientos para causar daño o beneficio personal. Se sustenta en cuatro pilares fundamentales:

Hacking Ético

Utilizar habilidades técnicas para identificar y corregir fallas mediante pruebas de penetración —por ejemplo, en sistemas de control de accesos de un edificio corporativo— contando siempre con la debida **autorización previa**.

Confidencialidad y Privacidad

Proteger la información personal y sensible de accesos no autorizados en todo momento, respetando los datos descubiertos en auditorías **incluso si nadie está vigilando**.

Transparencia y Responsabilidad

Comunicar de manera clara y asumir las consecuencias de las acciones profesionales, informando de inmediato a la dirección sobre cualquier brecha detectada bajo la propia guardia.

Cumplimiento de Normas

Respetar de forma irrestricta las regulaciones y directrices de protección de datos en todos los proyectos, **aun cuando el cliente no lo exija explícitamente**.

Cumplimiento Normativo y Marcos Legales

El ecosistema normativo de la ciberseguridad abarca regulaciones internacionales y leyes nacionales que las organizaciones deben cumplir para mitigar riesgos, evitar sanciones y proteger su reputación empresarial.

Marcos Internacionales

RGPD (Unión Europea)

Protege los datos de ciudadanos europeos y regula su tratamiento por parte de empresas en todo el mundo.

ISO 27001

Norma internacional reconocida globalmente que proporciona los estándares para la gestión de la seguridad de la información.

Políticas Internas

Reglas corporativas específicas para empleados, como las políticas de uso aceptable de recursos tecnológicos.

Marcos Legales en Chile

Ley Nº 21.663 (Marco de Ciberseguridad)

Publicada en 2024. Obliga a empresas del Estado, Prestadores de Servicios Esenciales (PSE) y Operadores de Importancia Vital (OIV) —bancos, telecomunicaciones, agua, salud— a mantener estándares estrictos y reportar ciberataques obligatoriamente.

Ley Nº 21.719 (Protección de Datos)

Regula la recolección, almacenamiento y resguardo de datos ciudadanos (RUT, dirección, tarjetas), otorgando los derechos ARCO+P: Acceso, Rectificación, Cancelación, Oposición y Portabilidad.

Autoridades Fiscalizadoras en Chile

ANCI

Agencia Nacional de Ciberseguridad. Dicta normas técnicas, audita empresas críticas y aplica multas de hasta **40.000 UTM** por faltas gravísimas.

CSIRT Nacional

Brazo técnico y operativo al que se deben reportar los ciberataques de manera obligatoria para coordinar la respuesta técnica nacional.

Agencia de Protección de Datos

Vigila que no se filtren datos privados, con facultades para iniciar investigaciones de oficio y sancionar la negligencia empresarial.

Casos Prácticos de Aplicación Legal en Chile

La teoría cobra vida real en estos dos escenarios críticos que ilustran las consecuencias legales concretas de no cumplir con la normativa vigente en Chile. Conocerlos es parte esencial de la formación.

⏱️ El Reloj de las 3 Horas — Ley 21.663

Ante un incidente de malware detectado a las 02:00 AM en una infraestructura crítica —como una empresa de distribución de agua potable—, la ley exige enviar una **Alerta Temprana al CSIRT Nacional en un plazo máximo de 3 horas**. El silencio organizacional u ocultar el ataque constituye un acto ilegal altamente sancionado.

🏥 Filtración de Datos en una Clínica — Ley 21.719

Si un ataque de phishing extrae una planilla con historiales médicos y RUN de **5.000 pacientes**, se debe notificar obligatoriamente a la Agencia de Protección de Datos sin dilaciones indebidas. La falta de controles básicos —como no exigir Doble Factor de Autenticación (MFA)— arriesga **multas millonarias o un porcentaje de la facturación anual** por negligencia.

¿Listo para convertirte en un profesional de la ciberseguridad? La **Escuela de Seguridad Privada** te entrega las herramientas, el conocimiento y el respaldo legal para proteger lo que más importa en el mundo digital.

Inscríbete al Curso | Contactar a la Escuela

Información de Pago y Contacto

En la Escuela de Seguridad Privada, nos esforzamos por ofrecerte la mayor flexibilidad y comodidad. A continuación, encontrarás nuestros métodos de pago, datos de contacto y horarios de atención.

Métodos de Pago Flexibles

- Efectivo
- Transferencia bancaria
- Tarjeta de crédito
- Crédito directo con la escuela

Nuestra Ubicación

Agustinas 972, Oficina 401, Santiago Centro

Contáctanos Directamente

- **www.escueladeseguridad.cl**
- **info@escueladeseguridad.cl**
- WhatsApp: +56 9 6591 6100

Horarios de Atención

- Presencial: Lunes a Viernes, 09:00 – 17:00 hrs
- WhatsApp: Lunes a Domingo, 08:00 – 23:00 hrs

¡Estamos aquí para ayudarte en cada paso de tu camino profesional! No dudes en contactarnos para cualquier consulta.