

Ciberseguridad en 25 horas

Una guía para aprender, practicar y mejorar tu seguridad digital

Pensado para **autodidactas, docentes y alumnos**
de Formación Profesional para el Empleo

© Francisko Parejo M.

Prólogo

Estimado lector:

*Me complace darte la bienvenida a **Ciberseguridad en 25 horas**, una guía práctica pensada para ayudarte a comprender los fundamentos de la ciberseguridad de forma clara, ordenada y accesible.*

Vivimos en un mundo cada vez más conectado. Usamos internet para comunicarnos, trabajar, estudiar, comprar, guardar información y gestionar buena parte de nuestra vida diaria. Sin darnos cuenta, dependemos de sistemas informáticos que deben ser seguros para proteger nuestros datos, nuestra privacidad y, en muchos casos, la actividad de empresas y organizaciones.

El propósito de este libro es ofrecerte una base sólida sobre los conceptos esenciales de la ciberseguridad. A lo largo de sus capítulos veremos qué riesgos existen, cómo actúan algunas amenazas habituales y qué medidas podemos aplicar para reducir los peligros. También hablaremos de políticas de seguridad, protección de la información, control de accesos, seguridad física y lógica, prevención y gestión de riesgos.

Mi objetivo es que este libro sea un compañero útil para quienes desean iniciarse en la ciberseguridad: estudiantes, profesionales que quieren reforzar sus conocimientos o personas interesadas en proteger mejor su entorno digital. En cada capítulo encontrarás explicaciones sencillas, ejemplos y ejercicios prácticos que te ayudarán a aplicar lo aprendido.

Este libro puede leerse de forma autónoma o utilizarse como material de apoyo en acciones formativas relacionadas con la seguridad informática.

La ciberseguridad cambia constantemente. Aparecen nuevas amenazas, nuevas herramientas y nuevas formas de trabajar. Por eso, más que memorizar conceptos aislados, es importante aprender a pensar con criterio, identificar riesgos y actuar con sentido común.

Te animo a recorrer estas páginas con curiosidad y espíritu práctico. No necesitas ser especialista para empezar. Lo importante es comprender los fundamentos y avanzar paso a paso.

¡Espero que este libro te resulte útil y que disfrutes del camino!

Porque en ciberseguridad, las personas no son solo el punto más vulnerable: también pueden ser la mejor defensa.

Una introducción clara y práctica a los fundamentos de la ciberseguridad, útil para el autoaprendizaje y para cursos de hasta 30 horas.

También puede servir como punto de partida para itinerarios más avanzados o formaciones técnicas más extensas.

... ÍNDICE ...

| | |
|-----------------------------------------------------------------------------|-----------|
| 1. Fundamentos..... | 11 |
| 1.1 Fundamentos de la Seguridad..... | 12 |
| ▪ Tipos de Información que se manejan..... | 14 |
| Práctica I (a): Escenario de seguridad en una empresa virtual..... | 16 |
| 1.2 Riesgos..... | 17 |
| ▪ Riesgos en la vida diaria..... | 17 |
| ▪ Cómo identificar y analizar riesgos..... | 19 |
| ▪ Amenazas habituales..... | 20 |
| ▪ Inyección SQL, XSS y clickjacking..... | 23 |
| ▪ Riesgo asumible: no todo riesgo se puede eliminar..... | 25 |
| Práctica I (b): Análisis de riesgos en un escenario empresarial..... | 26 |
| 1.3 Amenazas..... | 27 |
| ▪ Malware: cuando el problema está en el software..... | 27 |
| ▪ Phishing: cuando el ataque empieza con un engaño..... | 29 |
| ▪ Cómo protegerse frente al phishing..... | 30 |
| Práctica II (a): Identificación de correos de phishing..... | 32 |
| Práctica II (b): Creación de correos de phishing..... | 32 |
| ▪ Ciclo de vida de un ciberataque..... | 33 |
| ▪ Ataques de denegación de servicio: cuando el objetivo es interrumpir..... | 34 |
| ♣ Características clave de un ataque DDoS..... | 36 |
| 1.4 Seguridad básica al navegar por internet..... | 37 |
| ▪ ¿Qué son las cookies y cuál es su función?..... | 38 |
| ▪ Cómo protegerse de posibles amenazas..... | 39 |
| ▪ Ventanas privadas, modo incógnito o navegación privada..... | 39 |
| 2. Políticas de Seguridad Informática..... | 43 |
| 2.1 Gestión de la ciberseguridad..... | 43 |
| ▪ De la teoría a la práctica: ¿cómo se gestiona la ciberseguridad?..... | 44 |
| ▪ Evaluación de riesgos..... | 47 |
| ▪ Una fórmula sencilla para entender el riesgo..... | 50 |
| ▪ Ciberseguros: transferir parte del riesgo..... | 53 |
| ▪ Elaborar un Plan de Respuesta a Incidentes de Ciberseguridad..... | 54 |
| Práctica III (a): Plan de Respuesta a Incidentes..... | 62 |
| Práctica III (b): Plan de Respuesta a Incidentes. Ampliación..... | 63 |
| ▪ Respuesta ante incidentes personales..... | 63 |
| 2.2 Políticas de Seguridad..... | 64 |
| ▪ ¿Para qué sirven las políticas de seguridad?..... | 64 |
| ▪ Componentes básicos de las políticas de seguridad..... | 65 |
| ▪ Relación segura con proveedores, clientes y terceros..... | 66 |
| 2.2.1 Norma ISO 27001: SGSI..... | 67 |
| ▪ Pasos básicos para identificar y gestionar riesgos..... | 68 |
| Práctica IV (a): Creación de una Política de Seguridad..... | 71 |

| | |
|--------------------------------------------------------------------------------|------------|
| 2.3 Medidas de protección..... | 72 |
| ▪ Capas básicas de protección..... | 72 |
| Práctica IV (b): Diseño de Estrategias de Protección Cibernética..... | 77 |
| 2.3.1 Uso y creación de contraseñas seguras y robustas..... | 81 |
| ▪ Consejos para crear contraseñas seguras..... | 82 |
| ▪ Medidas que refuerzan la seguridad de tus contraseñas..... | 83 |
| ▪ Herramientas en línea para evaluar contraseñas..... | 85 |
| 2.4 Seguridad y respaldo de datos..... | 89 |
| ▪ Tipos de copias de seguridad..... | 89 |
| ▪ Copias de seguridad frente a ransomware..... | 94 |
| Práctica V: Plan de Copias de Seguridad Personal..... | 94 |
| ▪ Borrado seguro y gestión de soportes..... | 95 |
| ▪ Hoja de ruta básica para una empresa pequeña..... | 96 |
| 3. Seguridad en equipos, redes y dispositivos..... | 97 |
| 3.1 Control de acceso..... | 98 |
| Práctica VI: Implementación de políticas de control de acceso..... | 100 |
| 3.1.1 Compartir recursos sin abrir la puerta a todo el mundo..... | 100 |
| 3.2 Seguridad de redes Wi-Fi y protocolos de seguridad..... | 102 |
| ♣ Cifrado en redes Wi-Fi..... | 104 |
| ▪ Red de invitados Wi-Fi..... | 106 |
| ▪ Medidas para fortalecer la seguridad en redes Wi-Fi..... | 110 |
| Práctica VII: Revisión de seguridad Wi-Fi y contraseñas..... | 111 |
| ▪ Seguridad básica en dispositivos móviles..... | 112 |
| 3.3 Amenazas y software dañino..... | 113 |
| ▪ ¿Cómo nos protegemos de estas amenazas?..... | 113 |
| 3.4 Dispositivos <i>tamper-proof</i> | 116 |
| ▪ Diseño de un sistema de seguridad <i>tamper-proof</i> | 118 |
| 3.5 ♣ Side channel analysis..... | 119 |
| 3.6 ♣ Software Defined Radio y Cognitive Radio Networks..... | 121 |
| ▪ Ataques de interferencia o inyección de señales en redes Wi-Fi..... | 123 |
| 4. Acceso remoto..... | 125 |
| 4.1 Acceso remoto: usuarios, trabajadores y sedes..... | 126 |
| ▪ 1. Uso personal: navegar con más privacidad..... | 126 |
| ▪ 2. Uso como trabajador: acceder a la empresa desde fuera..... | 128 |
| ▪ 3. Uso en pequeñas empresas: conectar trabajadores, oficinas y recursos..... | 129 |
| ▪ 4. Una organización con varias sedes que necesita conectar redes..... | 130 |
| ▪ Acceso remoto al escritorio: VPN, herramientas externas y seguridad..... | 131 |
| 4.2 Demostración práctica de redes privadas virtuales..... | 133 |
| Escenario I: VPN para navegar por Internet con más privacidad..... | 133 |
| Escenario II: VPN para Teletrabajo..... | 133 |
| ♣ Otras formas avanzadas de proteger el acceso remoto..... | 134 |
| ▪ Comparativa entre herramientas de acceso remoto..... | 136 |

| | |
|-------------------------------------------------------------------------|------------|
| 5. Control de acceso a aplicaciones..... | 137 |
| 5.1 Autenticación y autorización en servicios web..... | 138 |
| 5.2 Passkeys: iniciar sesión sin contraseña..... | 140 |
| ▪ ¿Qué pasa si pierdo el móvil o cambio de ordenador?..... | 141 |
| 5.3 OAuth, OAuth2 y tokens..... | 142 |
| 5.4 Errores habituales en autenticación y autorización..... | 148 |
| 6. Aspectos legales..... | 149 |
| 6.1 Aspectos jurídicos en entornos tecnológicos..... | 150 |
| 6.2 Protección de datos y control de acceso..... | 152 |
| ▪ Aplicación práctica en una pequeña empresa..... | 153 |
| ▪ Brechas de seguridad: qué hacer si algo sale mal..... | 154 |
| ▪ Sanciones: por qué no conviene tomárselo a la ligera..... | 155 |
| ▪ Derechos digitales en el entorno laboral y personal..... | 156 |
| 6.3 ¿Quién es quién en protección de datos?..... | 157 |
| ▪ El Registro de Actividades de Tratamiento..... | 159 |
| 6.4 LSSICE: obligaciones básicas de servicios por Internet..... | 161 |
| ▪ Firma electrónica y servicios de confianza..... | 164 |
| 6.5 Protección intelectual y licencias..... | 166 |
| ▪ Software sin licencia, software libre y alternativas legales..... | 168 |
| ▪ Marcas, patentes, diseños y secretos empresariales..... | 170 |
| 6.6 Protección frente a código malicioso..... | 171 |
| ▪ ¿Qué ocurre si un malware provoca una brecha?..... | 171 |
| ▪ Medidas razonables, no seguridad perfecta..... | 172 |
| ▪ Sanciones y responsabilidad..... | 172 |
| Práctica VIII: ¿Un ransomware puede convertirse en una brecha de datos? | 173 |
| ANEXOS..... | 175 |
| I: GLOSARIO..... | 175 |
| II: Estrategias de Protección para Comercio Electrónico..... | 183 |
| III: Plan de Copias de Seguridad para la Empresa XYZ..... | 187 |
| IV: Direcciones IP, máscaras, MAC, DNS y DHCP..... | 191 |
| V: Técnicas avanzadas de búsqueda y revisión de huella digital..... | 193 |
| VI: Herramientas web y utilidades..... | 197 |