Sommaire :

- Protocoles sécurisés (SSL/TLS, IPsec, VPN)
- Pare-feu, filtrage, IDS/IPS
- Sécurité des communications

Chapitre 7. Identités, annuaires et habilitations

- Gestion des accès (authentification, autorisation)
- LDAP, Active Directory
- Contrôle des privilèges

Partie 3 : Politiques de sécurité du système d'information

Chapitre 8. Charte des utilisateurs

- Bonnes pratiques d'usage
- Sensibilisation à la sécurité
- Responsabilités des utilisateurs

Chapitre 9. Charte de l'administrateur système et réseau

- Rôles et responsabilités
- Gestion des incidents
- Bonnes pratiques techniques

Chapitre 10. Politique de sécurité des SI (PSSI)

- Élaboration d'une politique de sécurité
- Normes et référentiels (ex : ISO 27001)
- Gestion des risques et audit

Partie 4 : Avenir de la sécurité informatique

Chapitre 11. Nouveaux protocoles et nouvelles menaces

- Évolution d'Internet
- Cloud computing, IPv6
- Nouvelles surfaces d'attaque

Chapitre 12. Tendances des pratiques de sécurisation

- Gouvernance de la sécurité
- Automatisation et supervision
- Approche globale de cybersécurité

Chapitre 13. Cybersécurité et dimension géostratégique

- Cyberconflits
- Enjeux politiques et économiques
- Cas réels (attaques étatiques, crises Internet)
- Conclusion

- Bibliographie
- Index