
LA SÉCURITÉ INFORMATIQUE

- OBJECTIFS** ➤ Apporter une bonne connaissance de l'ensemble des concepts en matière de sécurité informatique par un enseignement basé sur de nombreux exemples et mises en situation réelles
- CONTENU**
- Introduction
 - Définitions et glossaire
 - Analyse de la sécurité informatique
 - Historique et situation actuelle
 - Aspect législatif
 - Évaluation des risques
 - Méthodes d'études de risques
 - Analyse des pertes directes et indirectes
 - Les risques physiques : électricité, eau, feu, accès aux locaux
 - Le piratage :
 - Les acteurs : Hacker, Cracker
 - Les logiciels et les matériels : scanner, sniffers, perceurs de mots de passe,
 - Virus et compagnie
 - Définitions et fonctionnement
 - Logiciels espions, spam, bombing
 - Anti-virus et protections : firewall, DMZ
 - Sécurité sur un réseau
 - Retour sur le modèle ISO : sécurité des différentes couches, cryptage, authentification, serveur proxy et filtrage
 - IP V4, IP V6, IPSec
 - Aspect juridique
 - Lexique, documentation et liens
- PÉDAGOGIE**
- Présentation théorique, mise en situation et études de cas, exercices pratiques
 - Chaque stagiaire disposera d'un micro-ordinateur PC Pentium connecté à INTERNET par ligne à haut débit (ADSL)
 - Chaque stagiaire recevra un document pédagogique