



Cycle Responsable Cybersécurité

Lien : <https://innov-maroc.com/formation/cycle-responsable-cybersecurite>

 DURÉE
10 jours (70h)

 RÉFÉRENCE
SEC01

 CATÉGORIE
**Cycles Métiers Sécurité
Informatique**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- ✓ Connaître les différents facteurs et typologies de risques
- ✓ Connaître les principes et les normes de chaque domaine de la SSI
- ✓ Être en mesure de sécuriser le réseau, le cloud et les applications
- ✓ Être en mesure d'effectuer des choix techniques
- ✓ Savoir élaborer un plan de secours et de continuité

POUR QUI ?

- ✓ Administrateurs
- ✓ Architectes
- ✓ Développeurs
- ✓ DSI
- ✓ Responsable sécurité

INNNOV MARROC



Programme détaillé

1 / Vue d'ensemble de la sécurité du Système d'Information

- Définitions et concepts fondamentaux
- Les composants de la cybersécurité : que faut-il protéger ?
- Défense en profondeur et politique de sécurité
- Principales méthodes (EBIOS, Mehari, ISO 27001...)
- La cybercriminalité
- Les menaces physiques
- L'analyse de risque
- Audits de sécurité : Les bonnes pratiques

2 / Sensibiliser et communiquer

- Plan de sensibilisation et de communication
- Charte de sécurité
- Couverture des risques
- Conception des solutions optimales : démarche
- IDS ou IPS
- Déploiement d'un projet PKI
- Les principes juridiques relatifs au SI
- Recommandations

3 / Sécurité du réseau

- Rappels sur le protocole TCP/IP
- Différents types de réseaux : VPN SSL, VPN IPsec, MPLS, VLANs, Wifi...
- Évolutions des menaces et les risques
- Systèmes de détection et de prévention des intrusions
- Sécurité des postes clients
- Sécurité du sans-fil
- Equipements : NAT, pare-feux, proxies, UTM...
- Méthodes et outils pour l'identification, l'authentification
- Éléments de cryptographie
- Sécurité pour l'Intranet/Extranet
- Les protocoles SSL
- Les meilleures pratiques pour superviser le réseau
- VPN. IPSec

4 / La sécurité dans le cloud

- Plan d'infrastructure technique pour les centres de données
- DMZ, VLANs et appliances next génération
- Plan de Continuité d'Activité (PCA)
- Plan de Reprise d'Activité (PRA)
- Etablir une stratégie de sauvegarde et d'archivage des données
- Critères d'externalisation pour virtualiser serveurs, réseaux et applications
- VPC, CASB, VPN...
- Cloud Control Matrix : analyser le risque
- Contrats et certifications d'hébergement

5 / Sécurité des logiciels et applications

- Différents techniques d'attaque des applications
- Les bonnes pratiques de développement
- Vue d'ensemble des outils de revue de code orientés sécurité
- La supervision active de la sécurité

- RSSI: ses missions dans le suivi de la sécurité
- Tour d'horizon sur les outils Sondes IDS, Scanner VDS, Firewall IPS
- Se tenir informé des nouvelles vulnérabilités
- Gestion des mises à niveaux
- Analyse de risques
- Bref présentation des terminologies ISO 27000
- Identifier et classer les risques

6 / L'analyse de risques selon l'ISO

- EBIOS 2010 et MEHARI 2010
- Choix de la meilleure méthode
- Une méthode globale ou une méthode par projet
- Coût d'une analyse de risques

7 / Plan de continuité, reprise d'activités (PCA/PRA) et plan de secours

- Les processus de la continuité d'activité
- Les différents plans : PCA/PRA, PCO, PSI, PGC, PCOM, ...
- La norme BS 25999 et le modèle BCI
- Les différentes phases d'un programme de continuité de l'activité
- Le plan de la continuité de l'activité

Approche pédagogique

- ✓ Support Ecrit et Projection
- ✓ Exposés Interactifs, Podcasts et Vidéos
- ✓ Brainstorming et Jeux de Rôle
- ✓ Cas Pratiques et Labs inclus pour leur impact opérationnel
- ✓ Test de Validation des Acquis des Connaissances

Prochaines dates programmées

 23 Nov. au 04 Déc. 2026

 Distanciel

 Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

 **Téléphone** : +212 522 247 210

 **Email** : contact@innov-maroc.com

 **Web** : <https://www.innov-maroc.com>

Document généré le 12/10/2026 — Réf : SEC01
INNOV MAROC — Tous droits réservés