

Cybersécurité des Systèmes d'Information de Santé : Enjeux, Réglementation et Protection

Lien : https://innov-maroc.com/formation/cybersecurite-des-systemes-dinformation-de-sante-enjeux-reglementation-et-protection

DURÉE
8 jours (56h)

RÉFÉRENCE
CSM289

CATÉGORIE
Santé Digitale, Data & Technologies

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- Comprendre les enjeux de la cybersécurité appliquée aux systèmes d'information de santé.
- Identifier les principales cybermenaces pesant sur les établissements de santé et les données médicales.
- Mettre en place une gouvernance de la sécurité conforme aux normes et réglementations internationales.
- Réaliser une analyse des risques et définir un plan de traitement adapté aux environnements de santé.
- Sécuriser les données de santé, les infrastructures informatiques, les applications et les dispositifs médicaux connectés.
- Déployer des mécanismes efficaces de détection, de réponse et de gestion des incidents de cybersécurité.
- Élaborer des plans de continuité et de reprise d'activité afin d'assurer la résilience des services critiques.
- Organiser des audits de cybersécurité, des campagnes de sensibilisation et des contrôles de conformité.
- Exploiter les nouvelles technologies de cybersécurité, d'intelligence artificielle et de surveillance avancée.
- Définir des indicateurs de performance et piloter l'amélioration continue du système de management de la sécurité de l'information.
- Préparer les établissements aux audits réglementaires et aux exigences des autorités compétentes.
- Développer une expertise permettant de protéger durablement les systèmes d'information de santé, de garantir la confidentialité des données des patients et d'assurer la continuité des activités face aux cybermenaces.

INNOV MAROC

POUR QUI ?

- Responsables des Systèmes d'Information (DSI)
- Responsables de la Sécurité des Systèmes d'Information (RSSI)
- Directeurs des systèmes d'information hospitaliers
- Ingénieurs et administrateurs systèmes et réseaux
- Responsables cybersécurité
- Responsables protection des données (DPO)
- Responsables qualité et gestion des risques
- Ingénieurs biomédicaux
- Responsables des applications hospitalières et de la santé numérique
- Auditeurs en sécurité des systèmes d'information
- Consultants en cybersécurité, conformité et gouvernance IT
- Toute personne impliquée dans la conception, l'exploitation, la sécurisation, l'administration ou la gouvernance des systèmes d'information de santé souhaitant renforcer ses compétences en cybersécurité, conformité réglementaire et résilience numérique.

INNOV MAROC



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ EN SANTÉ

- Enjeux des systèmes d'information de santé (SIS)
- Menaces, vulnérabilités et panorama des cyberattaques
- Confidentialité, intégrité, disponibilité et traçabilité des données

2 / GOUVERNANCE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

- Politique de sécurité des systèmes d'information (PSSI)
- Gouvernance, rôles et responsabilités
- Gestion des actifs informationnels

3 / CADRE RÉGLEMENTAIRE ET NORMATIF

- ISO/IEC 27001, ISO 27799 et ISO 27005
- RGPD, NIS2, HDS, HIPAA (selon le contexte)
- Exigences des autorités de santé et conformité réglementaire

4 / GESTION DES RISQUES CYBER

- Identification et cartographie des risques
- Analyse des risques selon EBIOS RM, ISO 27005 et NIST
- Plans de traitement et priorisation des mesures

INNOV MAROC

5 / PROTECTION DES DONNÉES DE SANTÉ

- Classification des données sensibles
- Chiffrement, pseudonymisation et anonymisation
- Gestion des accès, des identités et des habilitations (IAM)

6 / SÉCURISATION DES INFRASTRUCTURES ET DES APPLICATIONS

- Protection des réseaux hospitaliers
- Sécurisation des serveurs, postes de travail et applications métiers
- Sécurité du cloud, des API et des dispositifs médicaux connectés

7 / DÉTECTION DES MENACES ET RÉPONSE AUX INCIDENTS

- Supervision SOC, SIEM et détection des intrusions
- Gestion des incidents et investigations numériques
- Élaboration d'un plan de réponse aux cyberattaques

8 / CONTINUITÉ D'ACTIVITÉ ET CYBERRÉSILIENCE

- Plans de continuité (PCA) et de reprise d'activité (PRA)
- Sauvegardes sécurisées et restauration des données
- Gestion des crises cyber et exercices de simulation

9 / SENSIBILISATION, AUDITS ET CONTRÔLES

- Culture de cybersécurité et formation des utilisateurs
- Audits techniques et organisationnels
- Tests de vulnérabilité, revues de conformité et plans d'amélioration

10 / TECHNOLOGIES ÉMERGENTES ET INNOVATION

- Intelligence artificielle appliquée à la cybersécurité
- Zero Trust, SASE et architectures sécurisées

INOV MAROC

- Blockchain, cybersécurité des objets connectés médicaux (IoMT) et télésanté

11 / PILOTAGE DE LA PERFORMANCE ET CONFORMITÉ

- Définition des KPI et tableaux de bord cybersécurité
- Reporting à la direction et gouvernance
- Amélioration continue du SMSI

12 / ÉTUDES DE CAS ET ATELIER PRATIQUE

- Analyse d'une cyberattaque sur un établissement de santé
- Élaboration d'une stratégie de protection d'un système d'information hospitalier
- Construction d'une feuille de route intégrant gouvernance, gestion des risques, conformité réglementaire, cybersurveillance et résilience opérationnelle

Approche pédagogique

- ✔ Support Ecrit et Projection
- ✔ Exposés Interactifs, Podcasts et Vidéos
- ✔ Brainstorming et Jeux de Rôle
- ✔ Mises en Situation pour faciliter l'assimilation
- ✔ Cas Pratiques et Labs inclus pour leur impact opérationnel
- ✔ Test de Validation des Acquis des Connaissances

Prochaines dates programmées

12 au 21 Jan. 2027	Présentiel - Casablanca
08 au 17 Mars 2027	Présentiel - Casablanca
03 au 12 Mai 2027	Présentiel - Casablanca
28 Juin au 07 Juil. 2027	Présentiel - Casablanca
23 Août au 01 Sep. 2027	Présentiel - Casablanca

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

INOV MAROC

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC — Tous droits réservés

INNOV MAROC