Intégrer la Cybersécurité dans la Gestion de Projets Numériques

Lien : https://innov-systems.com/formation/integrer-la-cybersecurite-dans-la-gestion-de-projets-numeriques

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC287**	**Sécurité du SI**

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes fondamentaux de la cybersécurité et leur application dans les projets numériques
- Savoir identifier, évaluer et maîtriser les risques de sécurité dès la conception des projets (approche “Security by Design”)
- Intégrer les exigences juridiques et réglementaires (RGPD, DORA, NIS2, Secret des affaires) dans la gouvernance des projets IT
- Concevoir et piloter des projets sécurisés dans des environnements hybrides (on-premise, cloud, mobilité)
- Développer une culture de la sécurité dans les équipes projets et auprès des prestataires

POUR QUI ?

- Chefs de projets IT, responsables techniques ou fonctionnels
- Managers et responsables de services numériques
- DSI, RSSI, responsables conformité ou qualité
- Rédacteurs de cahiers des charges ou AMOA impliqués dans des projets numériques

Innov Systems

Programme détaillé

1 / CONTEXTE ET ENJEUX DE LA SÉCURITÉ DANS LES PROJETS IT

- Panorama des menaces actuelles et des vulnérabilités liées aux projets numériques
- Impacts économiques, juridiques et réputationnels d'une faille de sécurité
- Évolution du rôle de la sécurité dans la transformation numérique

2 / RÉGLEMENTATION ET NORMES ENCADRANT LA SÉCURITÉ DES PROJETS

- RGPD, DORA, NIS2, ISO 27001 et autres cadres applicables
- Responsabilités du chef de projet, du prestataire et du donneur d'ordre
- Clauses de sécurité et de confidentialité dans les contrats
- Gouvernance de la sécurité dans le cycle de vie projet

3 / CULTURE DE LA SÉCURITÉ ET GESTION DES ACTEURS

- Sensibilisation des équipes projets
- Communication avec les métiers et la direction
- Intégration de la sécurité dans la gouvernance projet (comités, reporting, validation)

4 / MÉTHODOLOGIE D'ANALYSE DE RISQUES CYBERSÉCURITÉ

- Identification des actifs critiques et des dépendances
- Évaluation des impacts et probabilités
- Classification des risques selon leur criticité (matrice de risques)
- Outils et référentiels d'analyse (EBIOS RM, ISO 27005)

5 / DÉFINITION DES EXIGENCES DE SÉCURITÉ DANS LES PROJETS

- Définir les besoins en confidentialité, intégrité, disponibilité
- Spécifier les exigences de sécurité dès la phase de conception

Innov Systems

- Intégrer les contraintes légales et normatives dans le cahier des charges
- Rédiger un plan de sécurité projet (PSP)

6 / GESTION DE LA SÉCURITÉ DANS LES FOURNITURES ET PARTENARIATS

- Choisir et évaluer les prestataires sous l'angle sécurité
- Exigences de sécurité dans les marchés publics et les contrats IT
- Suivi et audit des partenaires techniques et fournisseurs cloud

7 / SÉCURITÉ BY DESIGN ET BY DEFAULT

- Principes et bénéfices de la sécurité dès la conception
- Intégration dans les méthodes agiles, DevOps et cycle en V
- Bonnes pratiques de conception sécurisée : API, IAM, cryptographie, logs

8 / CONTRÔLE ET VALIDATION DES LIVRABLES

- Mise en place d'indicateurs de conformité et de sécurité
- Tests de sécurité : audit de code, pentest, revues d'architecture
- Vérification de la conformité aux exigences et documentation de sécurité

9 / GESTION DE LA RECETTE ET DE LA MISE EN PRODUCTION

- Checklists de validation sécurité
- Contrôle des configurations et durcissement des environnements
- Plan de continuité et de reprise d'activité (PCA/PRA)
- Gestion des changements et des mises à jour sécurisées

10 / CYBERSÉCURITÉ ET CLOUD COMPUTING

- Enjeux et responsabilités partagées du modèle cloud
- Sécurité des données hébergées : chiffrement, segmentation, supervision
- Maîtrise des incidents et continuité d'activité dans le cloud

Inov Systems

- Gestion de la conformité (HDS, ISO 27017/27018, clauses contractuelles)

11 / SÉCURITÉ DU NOMADISME ET DU TÉLÉTRAVAIL

- Bonnes pratiques de sécurisation des postes et accès distants
- Gestion des identités, authentification forte et MDM
- Sensibilisation des utilisateurs nomades
- Cas pratiques : scénarios d’incidents liés à la mobilité

12 / CONTRÔLE CONTINU ET AMÉLIORATION DU NIVEAU DE SÉCURITÉ

- Suivi des indicateurs de sécurité et reporting
- Retours d’expérience et capitalisation
- Mise en place d’une boucle d’amélioration continue (PDCA)
- Élaboration d’un plan d’action post-formation

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

Innov Systems

Prochaines dates programmées

24 au 27 Nov. 2026	Distanciel
02 au 05 Fév. 2027	Présentiel - Casablanca
30 Mars au 02 Avr. 2027	Présentiel - Casablanca
25 au 28 Mai 2027	Présentiel - Casablanca
20 au 23 Juil. 2027	Présentiel - Casablanca

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

Réservation & Renseignements

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

Innov Systems — Tous droits réservés

Innov Systems