



Gestion de la Sécurité des Systèmes d'Information (SMSIISO 27001) en Environnement Portuaire

Lien :

<https://afrique-formation.com/formation/gestion-de-la-securite-des-systemes-dinformation-smsiiso-27001-en-environnement-portuaire>

 DURÉE
8 jours (56h)

 RÉFÉRENCE
POR242

 CATÉGORIE
**Numérique, Data et
Systèmes
d'Information Portuaire**

🎯 OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les principes et exigences de la norme ISO/IEC 27001:2022.
- ✓ Concevoir, mettre en œuvre et piloter un SMSI dans un environnement portuaire.
- ✓ Identifier et protéger les actifs informationnels critiques des infrastructures portuaires.
- ✓ Réaliser une analyse des risques et définir les mesures de traitement appropriées.
- ✓ Sécuriser les systèmes IT, OT, SCADA, PCS et TOS.
- ✓ Mettre en place une gestion efficace des incidents de cybersécurité et des plans de continuité.
- ✓ Préparer les organisations portuaires aux audits et à la certification ISO/IEC 27001.
- ✓ Renforcer la sécurité des fournisseurs et de la chaîne logistique numérique.
- ✓ Développer une culture de cybersécurité auprès des collaborateurs.
- ✓ Intégrer les enjeux liés au Cloud, à l'IoT et aux technologies émergentes.
- ✓ Mesurer la performance et améliorer continuellement le SMSI.
- ✓ Développer une expertise en gouvernance de la sécurité de l'information adaptée aux infrastructures portuaires critiques.

👥 POUR QUI ?

- ✓ Responsables de la sécurité des systèmes d'information (RSSI)
- ✓ Directeurs des systèmes d'information (DSI)
- ✓ Responsables cybersécurité des autorités portuaires
- ✓ Responsables de la conformité et de la gestion des risques
- ✓ Responsables des infrastructures IT, OT, SCADA et ICS
- ✓ Responsables des Terminal Operating Systems (TOS) et Port Community Systems (PCS)
- ✓ Responsables de la continuité d'activité (PCA/PRA)
- ✓ Responsables qualité, gouvernance et contrôle interne
- ✓ Cadres des autorités portuaires, terminaux et entreprises logistiques
- ✓ Toute personne impliquée dans la gouvernance, la protection, l'audit ou la gestion de la sécurité des systèmes d'information des ports, terminaux et infrastructures maritimes critiques.



Programme détaillé

1 / FONDAMENTAUX DU SMSI ET DE L'ISO/IEC 27001

- Principes de la sécurité de l'information : confidentialité, intégrité et disponibilité
- Architecture d'un Système de Management de la Sécurité de l'Information (SMSI)
- Exigences de la norme ISO/IEC 27001:2022 et articulation avec ISO 27002

2 / GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

- Politique de sécurité et gouvernance cyber
- Rôles et responsabilités des parties prenantes
- Intégration du SMSI dans la stratégie des autorités portuaires

3 / ANALYSE DES RISQUES ET CONTEXTE PORTUAIRE

- Identification des actifs critiques (IT, OT, SCADA, TOS, PCS)
- Méthodologies d'analyse et de traitement des risques
- Élaboration du registre des risques et critères d'acceptation

4 / MISE EN ŒUVRE DES CONTRÔLES DE SÉCURITÉ

- Contrôles de l'Annexe A de l'ISO/IEC 27001
- Gestion des accès, authentification et chiffrement
- Sécurisation des réseaux, des systèmes et des données

5 / SÉCURITÉ DES SYSTÈMES INDUSTRIELS ET PORTUAIRES

- Protection des environnements OT, ICS et SCADA
- Sécurisation des Terminal Operating Systems (TOS) et Port Community Systems (PCS)
- Segmentation réseau et défense en profondeur

6 / GESTION DES INCIDENTS ET RÉSILIENCE CYBER

- Détection, notification et traitement des incidents
- Plan de réponse aux cyberattaques
- Continuité d'activité (PCA) et reprise après sinistre (PRA)

7 / CONFORMITÉ, AUDIT ET CERTIFICATION ISO 27001

- Préparation aux audits internes et externes
- Gestion des non-conformités et actions correctives
- Processus de certification et amélioration continue

8 / GESTION DES FOURNISSEURS ET DE LA CHAÎNE D'APPROVISIONNEMENT

- Évaluation des risques liés aux prestataires
- Clauses contractuelles de cybersécurité
- Sécurisation des services externalisés et des partenaires

9 / SENSIBILISATION, CULTURE CYBER ET FACTEUR HUMAIN

- Programmes de sensibilisation des collaborateurs
- Prévention du phishing, de l'ingénierie sociale et des erreurs humaines
- Développement d'une culture de cybersécurité

10 / DIGITALISATION, CLOUD ET NOUVELLES MENACES

- Sécurité des environnements Cloud et hybrides
- IoT, intelligence artificielle et objets connectés portuaires

- Tendances émergentes en cybersécurité maritime

11 / INDICATEURS DE PERFORMANCE ET PILOTAGE DU SMSI

- Définition des KPI et tableaux de bord
- Suivi de la maturité du SMSI
- Revues de direction et amélioration continue

12 / ÉTUDES DE CAS ET DÉPLOIEMENT D'UN SMSI PORTUAIRE

- Analyse de cyberincidents dans des ports internationaux
- Élaboration d'une feuille de route de mise en conformité ISO/IEC 27001
- Conception d'un SMSI adapté à une autorité portuaire ou un terminal maritime

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

 30 Nov. au 09 Déc. 2026

 Présentiel - Casablanca

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

Réservation & Renseignements

 Téléphone : +212 522 247 210

 Email : contact@afrique-formation.com

 Web : <https://www.afrique-formation.com>

Afrique Formation