COMPLIANCE ET MANAGEMENT DES RISQUES : RSSI

INTITULE DU POSTE :
Cadre Gestionnaire de la Sécurité des Systèmes d'Information

INTITULE DU POSTE DU SUPERIEUR HIERARCHIQUE :
Chef de la Division Responsable Sécurité des Systèmes d'information (RSSI)

1. Finalité(s)

Participer à l'élaboration, le déploiement et la supervision de la mise en œuvre de la politique de sécurité SI et veiller sur sa conformité aux règlementations et normes en vigueur.

2. Missions

I. **Assurer la Gouvernance et la Conformité en matière de Sécurité SI.**
II. **Gérer les Risques et Assurer la Sécurité Opérationnelle.**
III. **Contribuer au pilotage de l'Architecture de Sécurité et à la Sensibilisation et la Formation des collaborateurs.**

3. Activités principales

I. Assurer la Gouvernance et la Conformité en matière de Sécurité SI :

- Veiller au respect de la gouvernance de la sécurité SI et au bon fonctionnement de ses instances ;
- Veiller à la conformité des systèmes d'information avec les lois et réglementations applicables (Loi 09-08, RGPD, loi 05-20, DNSSI, etc.).
- Élaborer et contrôler les politiques de sécurité internes, en coordination avec les équipes techniques et la direction.
- Superviser les audits de sécurité (audits annuels, audits avancés, audits des prestataires) et garantir la conformité continue avec les exigences réglementaires.
- Contribuer à l'élaboration du reporting réglementaire en matière de contrôle interne IT et SSI, en veillant à la transparence des actions menées.

II. Gérer les Risques et Assurer la Sécurité Opérationnelle :

- Mettre en œuvre des dispositifs pour l'évaluation et la gestion des risques SI, en identifiant et en anticipant les menaces potentielles.
- Analyser et suivre les risques et vulnérabilités des systèmes d'information à travers des activités de veille en cyber sécurité (Threat Intelligence).
- Assister dans la gestion des incidents de sécurité, en apportant une analyse technique et en coordonnant la réponse avec le dispositif maCERT et les équipes de sécurité opérationnelle.
- Optimiser les scénarios de risques (Use Cases) et participer à l'intégration des plateformes techniques de supervision et de sécurité.
- Suivre et piloter les plans d'action de remédiation issus des résultats des audits et contrôles, pour assurer la correction des failles de sécurité identifiées.

Agence Nationale des Ports – Direction Générale – DCH – ANP

III. Contribuer au pilotage de l'Architecture de Sécurité et à la Sensibilisation et la Formation des collaborateurs :

- Participer à l'élaboration et à la mise en œuvre de la stratégie globale de sécurité SI, en alignant les objectifs techniques avec les priorités organisationnelles.
- Contribuer à la conception et à la mise en œuvre des plateformes et de l'architecture de sécurité des systèmes d'information.
- Superviser la mise en œuvre et la maintenance des infrastructures et outils de sécurité SI, en garantissant leur efficacité à long terme.
- Mettre en place des actions de sensibilisation et de formation pour promouvoir la culture de la sécurité au sein des équipes et des collaborateurs.

4. Relations internes et externes

Relations internes :

- Les Directions centrales ;
- Les Directions des Ports et Régions.

Relations externes :

- Prestataires et fournisseurs ;
- Auditeurs externes ;
- Autorités nationales en matière de sécurité des systèmes d'information.

5. Profil requis

Formation de référence : Titulaire d'un diplôme d'Ingénieur d'état ou d'une formation supérieure en Informatique, Télécommunications ou Systèmes d'information (Bac+5 minimum).
Spécialité : Sécurité des SI ou cyber sécurité.
Certifications : de type COBIT, ITIL, CMMI, CISA, CISSP, CISM, GCES, CEH et dans les normes internationales suivantes serait un plus :

- **ISO/IEC 27001.** Systèmes de Management de la Sécurité de l'Information (SMSI)
- **ISO 22301.** Management de la Continuité d'Activité (SMCA)

Expérience : 2 ans minimum dans les métiers de l'audit des systèmes d'information ou en tant que consultant junior et avoir participé à des missions en rapport avec la sécurité du SI.

6. Compétences

Savoir :

- Bonne connaissance du système d'information, de l'urbanisation et de l'architecture du SI.
- Maîtrise des normes, référentiels et méthodologies SSI (ISO 27001/2, 27005, 22301, etc.).
- Connaissance approfondie des réglementations et lois en matière de sécurité des SI (loi 05-20, DNSSI, Loi 09-08…).
- Maîtrise des normes et procédures de sécurité SI (antivirus, cryptographie, serveurs, tests d'intrusion, KPI…).

Savoir- faire :

- Maîtrise des outils de sécurité des systèmes d'information, incluant les solutions de prévention, détection et gestion des risques.
- Aisance à utiliser les outils d'évaluation et de maîtrise des risques SI, en assurant une gestion proactive des vulnérabilités et menaces.

- Assurer la gestion des risques en utilisant des méthodologies adaptées (tests d'intrusion, gestion des vulnérabilités, etc.).
- Évaluer et gérer les incidents de sécurité, en appliquant des protocoles standards et des outils de sécurité adaptés.
- Élaborer des indicateurs de performance (KPI) pour mesurer l'efficacité des dispositifs de sécurité et leur conformité.

Savoir- être :

- Éthique et intégrité.
- Excellente capacité d'organisation.
- Rigueur et objectivité.
- Esprit d'analyse et de synthèse.
- Résistance au stress pour faire face à des situations de crises ;
- Curiosité et sens de la communication.
- Sens du travail en équipe.
- Flexibilité et adaptabilité.

Agence Nationale des Ports
Direction Générale
DCH
ANP