

CQP Ingénieur en CYBERSECURITE

L'**Ingénieur en Cybersécurité** garantit la cohérence technique et la pérennité du système d'information lors de ses évolutions tout en veillant à optimiser les ressources, les performances et les coûts.

Les missions principales d'un Ingénieur en cybersécurité

Identification des risques et définition de la politique de sécurité

- Réaliser des audits du système de sécurité, le plus souvent avec l'aide de prestataires.
- Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité.
- Définir et faire évoluer la politique de sécurité des systèmes d'information du Groupe (PSSI).
- Etablir un plan de prévention des risques informatiques et un plan de continuité d'activité (PCA) (ou plan de maintien en conditions opérationnelles du S.I.).
- Définir ou faire évoluer les mesures et les normes de sécurité (charte), en cohérence avec la nature de l'activité de l'entreprise et son exposition aux risques informatiques (nomadisme, BYOD (Bring your own device), transferts de données, transactions financières...).
- Choisir les dispositifs techniques les plus appropriés aux besoins de l'entreprise (firewall, programmes de back up, cryptographie, authentification...).
- Participer à la définition et au contrôle de la gestion des habilitations.
- Participer au comité des risques.

Mise en œuvre et suivi du dispositif de sécurité

- Faire appliquer les normes et standards de sécurité.
- Mettre en place les méthodes et outils de sécurité adaptés, et accompagner leur implémentation auprès des utilisateurs.
- Gérer les projets d'infrastructures sécuritaires.
- Elaborer et suivre des tableaux de bord des incidents sécurité.
- Superviser ou auditer les programmes de sauvegarde (back-up).
- Gérer les incidents sécurité et proposer des solutions pour rétablir rapidement les services.
- Définir les actions à mener afin de réparer les dommages causés au SI en cas de survenance d'un sinistre de sécurité SI (intrusion dans le système, contamination par un virus, défaillance d'un équipement...), mettre en œuvre le plan de reprise d'activité (PRA).
- Faire analyser les causes des incidents et consolider les mesures de sécurité.
- Faire tester régulièrement le bon fonctionnement des mesures de sécurité mises en place pour en détecter les faiblesses et les carences.
- Auditer le respect des normes de sécurité informatique imposées aux sous-traitants de l'entreprise.

CQP Ingénieur en CYBERSECURITE

Communication et formation sur les normes de sécurité

- Réaliser le référentiel de sécurité, l'actualiser régulièrement, en assurer la diffusion et veiller à son application.
- Définir les formations à réaliser, superviser la rédaction des supports de formation et en assurer la diffusion (principalement auprès du service informatique).
- Mettre en place des actions de communication (en concertation avec le responsable de l'exploitation informatique ou les Risk managers métiers) auprès des salariés de l'entreprise en cas de risque majeur ou de dommages au SI causés par une attaque ou par des dégâts matériels.

Veille technologique et réglementaire

- Assurer une veille technologique, de manière à garantir la sécurité logique et physique du système d'information.
- Assurer une veille réglementaire sur la protection des données personnelles.
- Identifier les nouveaux risques sur la sécurité du système d'information : apparition de nouveaux virus, lancement d'attaques informatiques sur le réseau mondial...
- Rechercher des solutions innovantes pour répondre aux problématiques induites par l'introduction d'une nouvelle technologie.
- Suivre les évolutions juridiques du marché en termes de sécurité informatique afin de garantir la conformité du SI au droit individuel et collectif.
- Rédiger des notes technologiques de sécurité.

Management des équipes de correspondants / ingénieurs sécurité

- Assurer le management hiérarchique de son équipe : objectifs, congés, entretiens annuels, besoins de formation...
- Définir les plannings ainsi que la participation à des projets transverses (notamment comités risques dans la banque).
- Suivre l'action des correspondants sécurité.
- Suivre le budget alloué à la sécurité informatique.
- Participer au choix et l'évaluation des sous-traitants (sélection des SSII ou cabinets conseil, participation à la rédaction de l'appel d'offre et au dépouillement des réponses, sélection et réception des candidats).

Suivi des actions et reporting

- Contrôler les tableaux de bord techniques des incidents de sécurité rencontrés (virus, intrusion)
- Assurer le reporting des problèmes de sécurité en estimant les pertes financières (pertes engendrées et coût de mise en place d'une parade).

CQP Ingénieur en CYBERSECURITE

Qualités et compétences requises d'un Ingénieur en cybersécurité

Compétences techniques

- Bonne connaissance de la stratégie de l'entreprise, de son organisation, de ses métiers, enjeux.
- Bonne connaissance du système d'information global, de l'urbanisation et de l'architecture du SI et des interfaces en applications.
- Maîtrise des normes et procédures de sécurité et des outils et technologies qui s'y rapportent : firewall, antivirus, cryptographie, serveurs d'authentification, tests d'intrusion, PKI, filtres...
- Connaissance des principaux prestataires du marché de la sécurité informatique (éditeurs, sociétés de service...).
- Bonne connaissance des réseaux et systèmes.
- Bonne connaissance des outils d'évaluation et de maîtrise des risques (EBIOS, ISO 27005...)
- Connaissance des méthodologies (ex : OSSTMM, OWASP...).
- Bonnes connaissances juridiques en matière de sécurité et de droit informatique.
- Connaissance des normes ISO (si l'entreprise dispose d'une certification) et/ou PCI/DSF (banques, grande distribution ou e-commerce).
- Maîtrise de l'anglais, car 90 % des documents relatifs à la sécurité sont rédigés en anglais.

Aptitudes professionnelles

- Sens de la confidentialité, intégrité et éthique car le responsable sécurité a accès à des informations sensibles et stratégiques pour l'entreprise.
- Rigueur, capacité d'anticipation et sens de la méthode afin de mettre en place des programmes de sécurité efficaces.
- Pédagogie pour expliquer aux utilisateurs les règles à respecter pour ne pas mettre en danger le système d'information de l'entreprise.
- Diplomatie, écoute, sens du dialogue, persuasion, pour convaincre les utilisateurs des risques encourus et du bien-fondé des procédures mises en place.
- Résistance au stress pour faire face à des situations de crise nombreuses et inattendues (intrusion, virus, problème de sécurité « matérielle » (incendies, fuites d'eau...) et à prioriser les actions à mener.
- Curiosité, car le responsable sécurité doit, en permanence, se tenir au courant des nouveaux risques et des nouvelles parades (virus et antidotes).
- Force de proposition pour faire évoluer la stratégie, ainsi que les pratiques.
- Capacité à travailler et à s'adapter à tous les niveaux d'interlocuteurs de l'entreprise en adaptant son langage et son niveau d'explication à la population avec laquelle il est amené à travailler.