CYBERSÉCURITÉ

ISO/IEC 27032 : Lead Cybersecurity Manager

5 jours (35h00) | CS001 | Num form : form-183 | Perfectionnement / Avancé

INFORMATIQUE / SÉCURITÉ IT / CYBERSÉCURITÉ

À l'issue de ce stage vous serez capable de :

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/CEI 27032 et le Cadre de Cybersécurité NIST
- Connaître l'objectif, le contenu et la corrélation entre l'ISO/CEI 27032 et le Cadre de Cybersécurité NIST ainsi qu'avec d'autres normes et cadres opérationnels
- Maîtriser les concepts, les approches, les normes, les méthodes et les techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'une organisation
- Savoir interpréter les lignes directrices de l'ISO/CEI 27032 dans le contexte spécifique d'une organisation
- Acquérir l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans l'ISO/CEI 27032 et le cadre de Cybersécurité NIST
- Maîtriser les compétences pour conseiller une organisation sur les bonnes pratiques de gestion de la cybersécurité.

Ce Contenu de formation est proposé par PECB

Niveau requis :

Une connaissance fondamentale sur la norme ISO/CEI 27032 et des connaissances approfondies sur la cybersécurité.

Public concerné :

- Professionnels de la cybersécurité
- Experts en sécurité de l'information
- Professionnels souhaitant gérer un programme de cybersécurité
- Responsables du développement d'un programme de cybersécurité
- Spécialistes des TI
- Conseillers spécialisés dans les TI
- Professionnels des TI souhaitant accroître leurs connaissances et compétences techniques

Programme :

Jour 1 - Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032

- Objectifs et structure du cours
  Normes et cadres réglementaires
  Notions fondamentales de la cybersécurité
  Programme de cybersécurité
  Lancer un programme de cybersécurité
  Analyser l'organisme
  Leadership

Jour 2 - Politiques de cybersécurité, management du risque et mécanismes d'attaque

- Politiques de cybersécurité
  Gestion du risque de la cybersécurité
  Mécanismes d'attaque

Jour 3 - Mesures de contrôle de cybersécurité, partage et coordination de l'information

- Mesures de contrôle de cybersécurité
  Partage et coordination de l'information
  Programme de formation et de sensibilisation

Jour 4 - Gestion des incidents, suivi et amélioration continue

- Continuité des activités
  Management des incidents de cybersécurité
  Intervention et récupération en cas d'incident de cybersécurité
  Conclusion de la formation
  Tests en cybersécurité
  Mesure de la performance
  Amélioration continue

Jour 5 - Examen de certification ISO/IEC 27032 Lead Cybersecurity Manager

Ce Contenu de formation est proposé par PECB