



NOUVEAU

Cybersécurité: prévention, protection et défense

La question n'est plus si une cyberattaque surviendra, mais quand. La cybersécurité est désormais un pilier de la gouvernance et un facteur clé de succès des projets. Il est maintenant impératif pour toute organisation d'être en mesure d'anticiper les menaces afin de protéger les actifs stratégiques et de ne pas compromettre ses activités, voire sa survie.

Dans un contexte de transformation numérique accélérée, les organisations, infrastructures critiques et projets financés par des bailleurs de fonds sont des cibles privilégiées. Cette formation vous permettra d'acquérir les connaissances et habiletés nécessaires afin de bien analyser les menaces, d'évaluer les risques et de prendre des décisions éclairées pour renforcer la sécurité et la résilience de vos activités. Vous apprendrez à intégrer la cybersécurité dans vos pratiques de gestion et à mobiliser vos équipes autour d'une culture de vigilance durable.

OBJECTIFS PRATIQUES

- ✓ **Comprendre** les menaces et leurs impacts potentiels sur vos projets et votre organisation.
- ✓ **Définir** une vision stratégique intégrant la cybersécurité et l'imputabilité des décisions dans la gouvernance.
- ✓ **Identifier, évaluer et prioriser** les risques cyber dans vos projets.
- ✓ **Élaborer** les politiques et plans de réponse adaptés.
- ✓ **Renforcer** la culture de cybersécurité au sein de vos équipes.

CLIENTÈLE CIBLE :

- Cadres, gestionnaires de projets, responsables de programmes et décideurs souhaitant intégrer la cybersécurité dans leurs décisions stratégiques.

DURÉE : 2 semaines

THÈMES ET CONTENUS

- **Panorama des menaces et tendances actuelles :** Identifier les principales menaces cybernétiques qui visent les organisations et leurs projets. Comprendre les modes opératoires des cybercriminels et leurs impacts potentiels sur la gouvernance, les opérations et la réputation.
- **Cybersécurité et gouvernance :** Clarifier le rôle stratégique des cadres dans la prévention et la gestion des cyber risques. Intégrer la cybersécurité à la planification stratégique et à la gestion globale de projets.
- **Gestion des risques cyber :** Mettre en place un processus d'identification, d'évaluation et de hiérarchisation des risques. Déterminer les mesures préventives et correctives adaptées à la nature des projets et des actifs protégés.
- **Conformité et obligations légales :** Se familiariser avec les lois, règlements et normes internationales (RGPD, ISO 27001, NIST) qui encadrent la cybersécurité et la protection des données. Adapter les politiques organisationnelles pour assurer la conformité.
- **Gestion de crise et continuité des opérations :** Élaborer et tester un plan de réponse aux incidents. Renforcer la cyber-résilience en assurant la continuité des activités critiques en cas d'attaque.
- **Sécurité dans les projets et la chaîne d'approvisionnement :** Intégrer des exigences de cybersécurité dès la conception des projets. Évaluer et sécuriser les relations avec les fournisseurs, partenaires et sous-traitants.

