Résilience : gestion de crise et continuité d'activité

FAIRE FACE AUX CYBER-CRISES, DEVELOPPER LA CYBER-RESILIENCE

NOUVELLE FORMATION

Objectifs

- Décrypter les spécificités des cyber-crises
- Mettre en place une cellule de crise spécifique cyber
- Déployer les process spécifiques à la cyber-crise
- Déjouer les pièges de la communication de crise

Publics

- RSSI
- Risk Manager
- Responsable PCA
- Membres titulaires et suppléants de la cellule de crise

Formation(s) complémentaire(s)

- Le Maintien en Condition Opérationnelle des dispositifs de continuité
- Maîtriser le cadre réglementaire pour gérer les risques liés aux données personnelles

DURÉE : 2 JOURS
PRIX : 1 480€ HT
DATES : 27-28 AVRIL / 16-17 JUIN / 24-25 SEPTEMBRE / 25-26 NOVEMBRE

Programme

Cyber-crise : présentation des principes et conseils pratiques (intervention de nos experts...)

- Présentation de typologies et impacts des cyberattaques sur l'activité
- Outils de prévention et limites
- Détection et réponses techniques appropriées

La gestion des crises cyber : quelle organisation spécifique mettre en place ?

- Présentation des principes de gestion de crises complexes
- Identification des procédures de gestion de cyber-crises
- Le rôle de la cellule de crise cyber
- La préparation des équipes

La législation cyber : des obligations croissantes

- Panorama des législations internationales, focus sur les OIV
- Identification des outils à mettre en place pour une gestion juridique efficace des cyber-crises

La communication de cyber-crise : adopter une communication de crise adaptée

- Les enjeux de la communication de crise (réputation – rôle des médias – évoluer dans l'ère 2.0)
- Les conséquences d'une absence de communication de crise
- Les principes et les pièges de la communication de crise

Cyber-résilience

- Devenir cyber-résilient
- Cas pratiques et retours d'experience