

[PCR10]

▪ Objectifs

- Comprendre les enjeux et principes du Plan de Continuité d'Activité (PCA) dans le contexte de la cybersécurité
- Élaborer et mettre en œuvre un PCA adapté aux risques cyber
- Savoir tester, maintenir et faire évoluer le PCA
- Connaître les bonnes pratiques pour assurer la résilience des activités en cas d'incident cyber

▪ Public visé

- RSSI | DSI
- Responsable PCA et Cellule de crise
- Consultants sécurité, Chefs de projets et toute personne impliquée dans la gestion des risques et la résilience informatique

▪ Prérequis

- Avoir des connaissances de base en sécurité de l'information

▪ Accessibilité aux personnes en situation de handicap

- Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com



Savoir manager un Plan de Continuité d'Activité en cas de crise cyber

Programme de formation

▪ Introduction à la continuité d'activité et à la cybersécurité

- Définitions, enjeux et cadre réglementaire
- Différence entre PCA, PCA, PCA, PCA et PCA

▪ Analyse des risques cyber et impact sur l'activité

- Identification des menaces et vulnérabilités
- Cartographie des risques cyber
- Analyse d'impact sur les processus métier

▪ Élaboration du plan de continuité d'activité

- Définition des scénarios de crise
- Priorisation des ressources critiques
- Mise en place des mesures de prévention et de mitigation
- Rédaction du plan de continuité

▪ Mise en œuvre et organisation

- Rôles et responsabilités
- Mise en place des procédures d'intervention
- Communication en situation de crise

▪ Tests, maintenance et amélioration continue

- Planification des tests
- Retour d'expérience et mise à jour du PCA
- Formation et sensibilisation

[PCR10] Savoir manager un Plan de Continuité d'Activité en cas de crise cyber



Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter
- Exercices pratiques (simulation d'incidents cyber, élaboration d'un plan de continuité adapté à un contexte spécifique)
- Remise d'un support pédagogique favorisant la transférabilité des acquis



Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation



Durée

2 jours
(14 heures)



Groupe de formation

De 3 à 10 participants



Langue

Français

Anglais



Mode de déploiement

Présentiel

Distanciel

E-learning



Modalités

Intra

Inter

Sur-mesure



Tarif

Sur devis

Non concerné

Sur devis

Demande de devis – Modalités et délais d'accès

- Pour toute demande intra, contacter le Training Center à l'adresse trainingcenter.ocd@orange.com ou au 06 87 05 79 34. Le délai moyen de mise en œuvre est d'environ 2 mois (hors demande urgente).

