Sensibilisation PCA/PRA

CYBERSÉCURITÉ

Objectifs	Comprendre les enjeux et les principes fondamentaux du Plan de Continuité d'Activité (PCA) et du Plan de Reprise d'Activité (PRA) - Être capable d'identifier les processus critiques et d'élaborer un plan cohérent face aux menaces (cyber, sinistres, défaillances techniques) - Mettre en oeuvre et tester efficacement les dispositifs de continuité dans des scénarios de crise simulés.
Participants	Responsables sécurité, responsables IT - DSI - chefs de projet - gestionnaires de crise - auditeurs - consultants SSI - responsables métiers impliqués dans la continuité d'activité - étudiants en cybersécurité ou gestion de crise
Prérequis	Notions de continuité d'activité - compréhension des dépendances critiques - gestion de la résilience opérationnelle capacité à documenter et tester des scénarios de reprise - planification.
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation.
Méthodes pédagogiques	Exposés interactifs et démonstrations - Travaux pratiques individuels et en groupe - Échanges d'expériences et de bonnes pratiques
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	4150 € HT
Durée	5 jour(s) - 35 heure(s)
Modalités et délais d'accès	Formations accessibles sous 15 à 20 jours suite à votre demande. Un entretien initial doit être prévu avant votre entrée en formation.

Code : NCI_ZYNOAP7X

Mis à jour le : 25 mars 2026

Programme :

Fondamentaux PCA/PRA et cadre normatif

Définitions : PCA, PRA, BCP, DRP, gestion de crise

Panorama des risques (cyberattaques, pannes, incendies, pandémie, etc.)

Principes de résilience, disponibilité, redondance

Normes et cadres : ISO 22301, ISO 27031, ITIL, NIST

Périmètre, gouvernance et rôles (Direction, IT, Métiers, Sécurité)

Cas pratique

Analyse d'incidents majeurs ayant déclenché un PCA/PRA (OVH 2021, NotPetya, inondations, etc.)

Identification des points de défaillance critiques dans une infrastructure type

Cartographie initiale des dépendances SI et métiers

Analyse d'impact métier (BIA) et scénarios de crise

Business Impact Analysis (BIA) : objectifs, méthodologie

Identification des activités critiques

RTO (Recovery Time Objective) et RPO (Recovery Point Objective)

Construction de scénarios de crise réalistes (attaque ransomware, sinistre datacenter, coupure réseau...)

Cas pratique

Réalisation d'une BIA sur un cas d'étude (entreprise e-commerce ou service public)

Évaluation des impacts métiers : pertes financières, image, juridique

Élaboration de 2 scénarios de crise à simuler dans les jours suivants

Élaboration du PCA et PRA

Elaboration du PCA : stratégie de continuité, ressources, procédures, sites de repli

Élaboration du PRA : stratégie de reprise, restauration SI, priorisation, documentation

Intégration des solutions techniques : réplication, sauvegarde, bascule automatisée

Rédaction des documents opérationnels (fiche réflexe, plan de communication, astreinte)

Cas pratique

Rédaction d'un plan PCA/PRA basé sur les scénarios du jour 2

Définition des procédures d'escalade, contacts clés, rôles de crise

Création de checklists automatisables (outils comme runbooks/scripts)

Simulation, tests, automatisation

Typologie des tests : à blanc, partiel, en réel, surprise

Outils de simulation de crise et gestion de logs (SIEM, observabilité)

Automatisation des PRA : infrastructure as code, déclenchement auto, DRaaS

Mesure de la résilience et indicateurs de performance

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon

Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille

www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20

Cas pratique

Création d'un test de bascule simulée (VMfailover, backup restore...)

Déclenchement d'un PRA simulé avec contraintes métiers

Mesure du respect des RTO/RPO, analyse des écarts

Exploitation des journaux pour validation

Atelier de crise et restitution

Atelier

Scénario global (à choix) :

Exemple 1 : attaque par ransomware sur serveurs critiques (AD, applicatif métier)

Exemple 2 : incendie dans un datacenter et indisponibilité réseau

Exemple 3 : compromission cloud avec perte de secrets et infrastructure détruite

Objectifs de l'atelier :

Réaction en temps réel (simulation de crise)

Activation du PCA ou PRA selon besoin

Suivi d'une cellule de crise (prise de décision, communication, reprise progressive)

Revue post-mortem : points forts, axes d'amélioration, mise à jour des plans

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20