Modèle de PCA/PRA sécurité électronique

Référence	Version	Date	Catégorie
MOD-CRM-006	v1.0	Février 2025	Commercial & Relation Client

> ***Modèle***

Ce modèle structure l'élaboration des Plans de Continuité d'Activité (PCA) et des Plans de Reprise d'Activité (PRA) spécifiques aux systèmes de sécurité électronique. Un système de sécurité défaillant peut exposer un site à des risques majeurs. La capacité à maintenir ou à rétablir rapidement les fonctions de sécurité essentielles est donc une priorité absolue pour les organisations dont la sécurité physique est critique.

---

01. Distinction PCA et PRA, périmètre couvert

Le Plan de Continuité d'Activité (PCA) vise à maintenir les fonctions de sécurité essentielles pendant un sinistre, avec un niveau de service dégradé mais opérationnel. Il répond à la question : comment continuer à assurer la sécurité du site malgré la défaillance d'un ou plusieurs composants du système ? Le Plan de Reprise d'Activité (PRA) vise à rétablir l'ensemble des fonctions de sécurité dans leur état nominal après un sinistre. Il répond à la question : comment revenir à un fonctionnement normal dans les meilleurs délais ?

Le périmètre couvert par le PCA/PRA comprend l'ensemble des systèmes de sécurité électronique déployés sur le site : vidéoprotection (serveurs VMS, NVR, infrastructure réseau vidéo, postes de visualisation), contrôle d'accès (serveurs, contrôleurs, lecteurs), détection intrusion (centrale d'alarme, transmetteurs), et hypervision (hyperviseur, tableau de bord de supervision). Les systèmes de sécurité des systèmes (onduleurs, alimentation secourue) sont également inclus dans le périmètre.

02. Scénarios de sinistre couverts

Trois scénarios de sinistre principaux sont traités dans le PCA/PRA. Scénario 1 — Incendie de la salle serveur ou du local technique : destruction totale ou partielle des équipements centraux (VMS, serveur de contrôle d'accès), avec maintien possible de certains équipements périphériques (caméras alimentées par PoE sur switches survivants, contrôleurs d'accès autonomes, centrale d'alarme sur batterie). Ce scénario est généralement le plus impactant et constitue le dimensionnement du PRA.

Scénario 2 — Cyberattaque (ransomware, destruction de données, prise de contrôle) : compromission des systèmes logiciels sans nécessairement de destruction matérielle. Ce scénario peut impliquer une déconnexion volontaire des systèmes du réseau pour limiter la propagation, avec basculement sur un mode de fonctionnement autonome (enregistrement local sur les caméras, contrôleurs d'accès en mode autonome). Scénario 3 — Panne matérielle majeure (disques de stockage, alimentation centrale, switch cœur de réseau vidéo) : défaillance d'un composant critique sans incident extérieur. C'est le scénario le plus fréquent et généralement le plus simple à traiter.

---

03. RTO et RPO par système

Pour chaque système et chaque scénario de sinistre, le PCA/PRA définit deux indicateurs clés : le RTO (Recovery Time Objective — délai maximum acceptable pour le rétablissement du service) et le RPO (Recovery Point Objective — perte de données maximale acceptable, exprimée en durée). Ces objectifs sont définis par le client en fonction de ses exigences opérationnelles et servent à dimensionner les solutions techniques de continuité et de reprise.

Des valeurs de RTO/RPO typiques pour les systèmes de sécurité électronique : vidéoprotection en mode consultation (RTO : 4 heures, RPO : 0 heure — les enregistrements en cours de la nuit précédente ne peuvent être perdus) ; contrôle d'accès en mode autonome (RTO : 1 heure — les portes doivent être contrôlées, même en mode dégradé) ; hypervision (RTO : 8 heures, RPO : 24 heures). Ces valeurs sont à valider et à ajuster avec chaque client.

---

04. Procédures de bascule et de restauration

Les procédures de bascule définissent les actions à réaliser immédiatement après la survenance d'un sinistre pour activer le mode de fonctionnement dégradé prévu par le PCA. Elles sont rédigées sous forme de fiches opérationnelles, utilisables par le personnel de sécurité du client sans expertise technique approfondie : chaque fiche couvre un scénario spécifique et liste les actions à réaliser dans l'ordre, avec les contacts à appeler à chaque étape.

Les procédures de restauration définissent les étapes de remise en service nominal après résolution du sinistre. Elles précisent : la séquence de réinstallation des systèmes (du plus critique au moins critique), les sources de restauration (sauvegardes, équipements de remplacement pré-positionnés, interventions Mileo Technology), les tests à réaliser pour valider la remise en service, et les modalités de communication vers le client et les utilisateurs tout au long de la restauration. Le PCA/PRA est testé annuellement lors d'exercices simulés et mis à jour après chaque incident réel ou changement significatif du système.

47 Boulevard de Courcelles, 75008 Paris — hello@mileotech.com