logiq

INTÉGRATEUR PREMIUM · CYBERSÉCURITÉ

LIVRE BLANC · 2026

Combien de temps votre entreprise peut-elle tenir à l'arrêt ?

PRA / PCA : le guide de la continuité d'activité. La méthode, le diagnostic, et les 5 erreurs qui font échouer un plan le jour J.

LOGIQE · INTÉGRATEUR PREMIUM · INFRASTRUCTURE · CYBERSÉCURITÉ · CLOUD & COLLABORATION

INTRODUCTION

La panne n'est plus une hypothèse. L'arrêt prolongé, si.

Une cyberattaque, une panne majeure, un système critique indisponible : ce n'est plus une question de « si », mais de « quand ». Et le jour où ça arrive, une seule chose compte vraiment : **combien de temps votre activité peut continuer à tourner**. Et à quelle vitesse vous redémarrez.

La plupart des organisations se pensent prêtes. Dans les faits, très peu disposent d'un plan de continuité réellement opérationnel. Le jour J, le résultat est toujours le même : une interruption qui s'éternise, des pertes financières, une image écornée, et des décisions prises dans l'urgence.

Ce livre blanc va droit au but : ce qu'est vraiment un PRA/PCA, comment le construire, et les erreurs qui transforment un « plan » en fausse sécurité.

1 / 5

PME touchée par une cyberattaque finit par fermer ou déposer le bilan.

SOURCE : ÉTUDE MASTERCARD

2 / 3

des PME ont subi une cyberattaque en France en 2025.

SOURCE : BAROMÈTRES CYBER 2025

dès 1 h

d'arrêt, la facture se chiffre déjà en dizaines de milliers d'euros.

SOURCE : ITIC / GARTNER

> *« Un PRA/PCA, ce n'est pas un classeur sur une étagère. C'est votre capacité à redémarrer. »*

SECTION 01

PRA, PCA : de quoi parle-t-on vraiment ?

PCA

Plan de Continuité d'Activité

Garder l'essentiel en marche **pendant** la crise. Objectif : aucune (ou quasi aucune) interruption sur les activités vitales de l'entreprise.

PRA

Plan de Reprise d'Activité

Remettre le système d'information debout **après** l'incident. Objectif : redémarrer vite, proprement, et dans le bon ordre.

RTO · Recovery Time Objective

La durée d'arrêt acceptable avant de redémarrer. **Combien de temps** peut-on rester à l'arrêt ?

RPO · Recovery Point Objective

Le volume de données qu'on accepte de perdre. **Jusqu'où** remonte la dernière sauvegarde utilisable ?

Ces deux chiffres pilotent tout le reste. Les fixer, c'est **traduire le risque en décisions concrètes** : budget, architecture, fréquence des sauvegardes, niveau de service.

1

Audit

Identifier les activités critiques, les dépendances et les points de rupture.

2

Plan

Définir les scénarios de crise et les stratégies de continuité et de reprise.

3

Tests

Vérifier que tout fonctionne réellement… avant le jour J, pas pendant.

4

Procédures

Donner aux équipes des actions claires à exécuter en cas d'incident.

SECTION 02

Les 5 erreurs qui font échouer un plan le jour J

Un plan jamais testé, c'est un parachute jamais plié : on ne découvre le problème qu'au moment du saut.

1 **Des procédures incomplètes**

Des étapes manquent, et personne ne sait quoi faire, ni dans quel ordre, quand le chrono tourne.

2 **Des rôles mal définis**

Au moment critique, chacun attend que quelqu'un d'autre décide. La crise se gère pendant la crise.

3 **Des délais (RTO/RPO) irréalistes**

On vise « quelques heures » avec des moyens calibrés pour « plusieurs jours ». L'écart se paie cash.

4 **Des sauvegardes jamais restaurées**

Une sauvegarde qu'on n'a jamais testée par une restauration réelle n'est pas une sauvegarde : c'est un espoir.

5 **Un plan obsolète**

L'infrastructure a changé, le plan non. Il décrit un système d'information qui n'existe déjà plus.

VU SUR LE TERRAIN

Un PRA existait, les sauvegardes étaient « en place ». Au premier vrai test : procédures incomplètes, rôles flous, délais intenables. **Résultat : plusieurs jours d'arrêt, là où quelques heures étaient attendues.**

SECTION 03

Êtes-vous vraiment prêt ? Le test en 8 questions

Cochez honnêtement. Chaque case vide est un point de fragilité le jour de l'incident.

- ☐ Nous avons identifié nos activités critiques et leurs dépendances.
- ☐ Les rôles et responsabilités en cas de crise sont écrits et connus de tous.
- ☐ Le plan a été testé grandeur nature au moins une fois cette année.
- ☐ Le plan est mis à jour à chaque changement majeur d'infrastructure.
- ☐ Un RTO et un RPO sont définis pour chaque activité critique.
- ☐ Nos sauvegardes sont testées par une restauration réelle, régulièrement.
- ☐ Les procédures restent accessibles même si le SI est totalement à terre.
- ☐ Un interlocuteur est joignable 24h/24 en cas d'incident.

Plus de 3 cases vides ? Votre continuité repose aujourd'hui sur la chance.

L'approche LOGIQE

Analyse des risques réels · Scénarios concrets · Tests réguliers · Accompagnement des équipes

Objectif : un plan réellement utilisable le jour où tout bascule. Pas un document pour « cocher une case ».

À noter : avec la directive **NIS2**, la continuité d'activité et la gestion de crise deviennent des obligations pour un nombre élargi d'organisations (entités essentielles et importantes). Anticiper, c'est se mettre en conformité tout en se protégeant.

Un intégrateur Premium, extension de votre DSI

LOGIQE est un **intégrateur Premium** en Cybersécurité, Systèmes & Réseaux, ITOM, Cloud & Collaboration. Notre métier : la gouvernance, l'intégration et l'exploitation de votre système d'information, avec un ADN sur-mesure et une logique de proximité. Concrètement, nous devenons l'**extension opérationnelle de votre DSI**, y compris le jour où tout bascule.

7
agences en France

3
implantations à l'international

+100
experts en infrastructure IT & cybersécurité

+70
certifications techniques

+70
solutions partenaires intégrées

+150 %
de croissance annuelle depuis 2021

3 M€ → 10 M€ De 3 M€ de chiffre d'affaires aujourd'hui à un objectif de 10 M€ en 2027. Une croissance au service des ETI et Grands Comptes.

Un positionnement unique

- **Analyse continue** des technologies émergentes à déployer.
- **Service client & delivery** d'excellence.
- **Offres sur-mesure**, un ADN « taylor made ».
- **Proximité & infogérance Premium**, extension de vos capacités IT.

RÉFÉRENCÉ SUR **CYBERMALVEILLANCE.GOUV.FR** · AU SERVICE DES ETI & GRANDS COMPTES

PASSEZ À L'ACTION

Évaluez votre préparation. Avant que l'incident ne le fasse à votre place.

30 minutes avec un expert LOGIQE pour identifier vos points de fragilité et la priorité n°1 à sécuriser. Sans jargon, sans sur-vente : un plan d'action clair, adapté à votre réalité.

Jim COUPEZ

Fondateur · Directeur Commercial & Avant-Vente

06 23 09 84 52

jim.coupez@logiqe.fr

Prendre rendez-vous

OUVERT 7J/7 · 24H/24

NOUS RETROUVER : 7 AGENCES EN FRANCE, 3 À L'INTERNATIONAL

Sophia Antipolis
230 Route des Dolines, 06560

Paris
47 Rue de Monceau, 75008

Lyon
3 Rue de Genève, 69006

Nantes
17 Rue Océane, 44800

Lille
2 Rue de l'Épine, 59650

Strasbourg
Ouverture 2026 · T1

Dubaï · UAE
World Trade Centre (DWTC)

Bangkok · Thaïlande
Gaysorn Tower, 127 Ratchadamri

Panama
Regus · Oceania, Punta Pacifica

logiqe

INTÉGRATEUR PREMIUM
INFRASTRUCTURE · CYBERSÉCURITÉ · CLOUD