PLANIFIER LA CONTINUITÉ DES AFFAIRES

Dans un monde de plus en plus incertain, la planification de la continuité des affaires ne peut pas se limiter qu'à des considérations purement technologiques. Elle doit s'appuyer sur une démarche globale, structurée et proactive, intégrant l'ensemble des fonctions critiques de l'organisation.

- Opérations
- Chaînes d'approvisionnement
- Ressources humaines
- Finances
- Légal
- Technologies de l'information

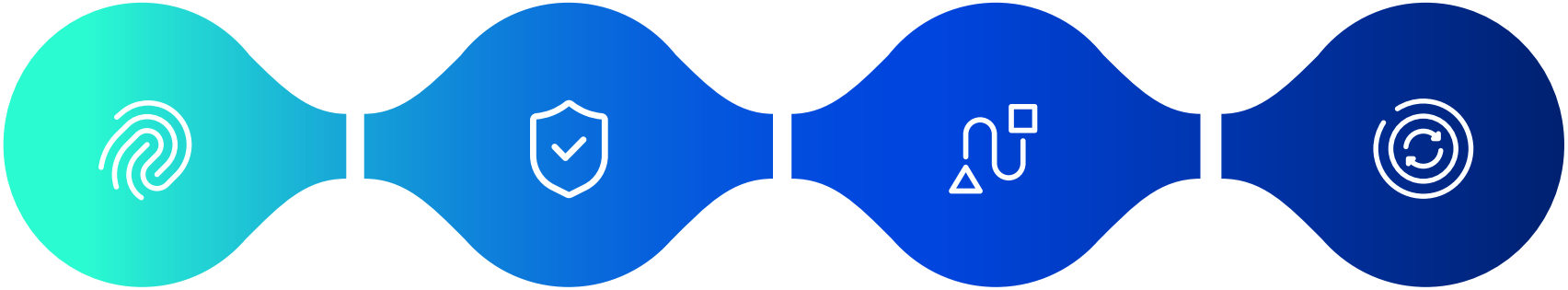
INTELLIGENCE TI.
INTELLIGENCE HUMAINE.

Parlons-nous

Sans frais 1-888-251-1622 **ITI Québec** 418-871-1622 **ITI Montréal** 514-940-1662 **ITI Toronto, Kingston et Ottawa** 1-866-549-6558

iti.ca

LES 4 PILIERS DE LA RÉSILIENCE ORGANISATIONNELLE



ÉTAPE 1
LA PRÉVENTION

Former les employés pour réagir efficacement avant, pendant et après une attaque.

+ MFA / Gestion d'accès
+ Mises à jour
+ Sécurisation des systèmes et des communications
+ Sauvegardes / solutions de recouvrement
+ Gestion d'accès
+ Tests d'hameçonnage
+ Tests d'intrusion internes et externes

ÉTAPE 2
LA DÉTECTION

Identifier l'événement, réduire les impacts et garantir une intervention efficace.

+ Systèmes de détection d'intrusion : Intrusion Detection Systems (IDS) et Intrusion Prevention Systems (IPS)
+ EDR (endpoint detection and response) pour ordinateurs et téléphones
+ MDR (managed detection response) pour l'ensemble des infrastructures TI, le nuage et les réseaux
+ Analyse comportementale : Détection des activités anormales
+ Surveillance de la disponibilité et des pannes des systèmes

ÉTAPE 3
LA RÉPONSE

Réagir rapidement, efficacement et de façon coordonnée.

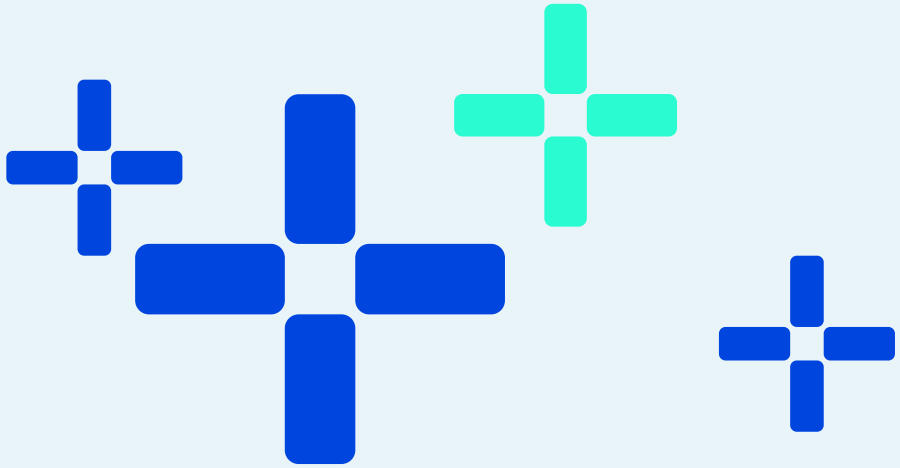
+ Exécution du *Plan de réponse aux incidents* (quoi faire, qui et quand)
+ Équipe de réponse aux incidents qui connaît les outils sensibles, le plan à suivre et les procédures de documentation
+ Plan de communication en situation de crise qui informe les employés sans créer de panique et gère la relation client, les médias et les partenaires

ÉTAPE 4
LA REPRISE

Réduire les impacts opérationnels, financiers et réputationnels.

+ Plan de reprise : document évolutif, restauration des systèmes critiques
+ Priorisation : cartographie des actifs vitaux (paiements, production, RH)
+ Communication : transparence interne et externe post-incident
+ Analyse post-mortem : identifier failles, améliorer procédures

PAR OÙ COMMENCER?



1 — EFFECTUER UN BILAN D'IMPACT SUR LES ACTIVITÉS (BIA)

Identifier les activités critiques de l'organisation et les ressources humaines et technologiques indispensables à leur fonctionnement. Évaluer les impacts financiers, opérationnels et réputationnels que des interruptions pourraient engendrer.

2 — METTRE EN PLACE LES STRATÉGIES

Déterminer les RPO (Recovery point objective) et RTO (Recovery time objective) en fonction du BIA. Mettre en place des outils adaptés, tels que des sauvegardes et des solutions de reprise après sinistre, pour garantir une protection efficace.

3 — ÉLABORER UN PLAN DE RÉPONSES AUX INCIDENTS (PRI)

Développer des procédures pour détecter, répondre et récupérer rapidement. Les conséquences et les impacts d'une inaction doivent aussi être mesurés ; perte de revenus, atteinte à la réputation, sanctions contractuelles ou réglementaires, etc.

4 — DÉVELOPPER UN PLAN DE REPRISE APRÈS SINISTRE (PRS)

Définir des stratégies précises visant à rétablir les systèmes et les données à la suite d'un sinistre, en tenant compte du niveau de criticité des activités.

5 — ORGANISER UN PLAN DE CONTINUITÉ DES ACTIVITÉS (PCA)

Créer un plan global pour maintenir les opérations essentielles pendant et après une interruption majeure.

6 — TESTER, MESURER ET AJUSTER

Les exercices de simulation et les retours d'expérience (post-mortem) sont essentiels pour vérifier l'efficacité d'un plan de continuité des affaires et pour entraîner les équipes à réagir en situation réelle.