Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Renforcement de la cyberrésilience grâce à une préparation en cas d'urgence

Série Gestionnaires

TLP:CLEAR

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour de plus amples renseignements, veuillez communiquer avec le Centre pour la cybersécurité :

- par courriel : contact@cyber.gc.ca
- par téléphone : 613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 15 janvier 2026.

Historique des révisions

Révision	Modifications	Date
1	Première version.	15 janvier 2026

ISBN 978-0-660-975443-3
CAT D96-136/2026F-PDF

Présentation

Votre plan de préparation en cas de cyberurgences offrira à votre organisation une stratégie pour prévenir les cyberincidents, y répondre et garantir une reprise efficace. La mise en œuvre d'une stratégie de préparation en cas de cyberurgences nécessite des efforts collaboratifs de la part des intervenants dans toute votre organisation. Votre stratégie devrait mettre en évidence les aspects importants de vos procédures d'intervention en cas d'urgence, comme les étapes à entreprendre pour répondre à un incident, les personnes à contacter dans une telle éventualité ainsi que les ressources qui seront nécessaires pour l'application générale de votre plan. Une stratégie de préparation en cas de cyberurgences aidera votre organisation à gérer les risques et à améliorer sa résilience dans l'éventualité d'une catastrophe.

La présente publication décrit une stratégie de préparation en cas de cyberurgences dans le contexte de la cybersécurité. Cette stratégie doit ainsi inclure un plan d'intervention en cas d'incident (PICI), un plan de continuité des activités (PCA) et un plan de reprise après sinistre (PRS). La différence entre ces trois plans est détaillée dans la publication, ainsi que les justifications pertinentes pour mettre au point et mettre en œuvre les trois plans. Cela vous permettra de renforcer votre cyberrésilience ainsi que vos capacités à maintenir vos activités en cas d'incident ou de perturbation majeure.

Votre plan de préparation en cas de cyberurgences doit être aligné avec le cadre de gestion des risques de sécurité que vous aurez choisi. Par exemple :

- Gestion des risques liés à la sécurité : Une méthode axée sur le cycle de vie (ITSG-33) du Centre pour la cybersécurité
- Cyber Security Framework du National Institute of Standards and Technology (NIST) (en anglais seulement)
- Sécurité de l'information, cybersécurité et protection de la vie privée – Mesures de sécurité de l'information du International Organization for Standardization (ISO)

L'intégration de votre plan de préparation en cas d'urgence au cadre de sécurité de votre organisation favorisera un renforcement de la cyberrésilience et une meilleure protection de la confidentialité, de l'intégrité et de la disponibilité de vos actifs organisationnels.

Nous vous recommandons de signaler les cyberincidents au Centre pour la cybersécurité à partir de notre outil de signalement en ligne. Nous pouvons fournir à votre organisation des conseils, des directives ainsi que des services en matière de cybersécurité afin de vous aider à atténuer les répercussions des cyberincidents actuels et de mieux vous protéger contre ceux qui pourraient survenir à l'avenir. Nous vous recommandons également de signaler les activités cybercriminelles à la police et les cas de fraude au Centre antifraude du Canada.

Table des matières

Liste des figures

1 Présentation des préparatifs d'urgence

Vous devez tenter d'améliorer la posture de sécurité et la résilience de votre organisation en vous préparant de manière proactive contre les incidents et les perturbations. De la sorte, vous pourrez anticiper et minimiser les temps d'arrêt, les pertes financières et les dommages à la réputation qui pourraient s'en suivre.

Votre stratégie de préparation en cas de cyberurgences doit comprendre trois types de planification complète :

- plan d'intervention en cas d'incident (PICI)
- plan de continuité des activités (PCA)
- plan de reprise après sinistre (PRS)

La présente publication se concentre sur les activités de préparation en cas d'urgence associées. En particulier, nous traiterons de la reprise et de la restauration des actifs technologiques (tangibles et intangibles) qui servent à l'exploitation de vos activités et qui risquent d'être négativement affectées en cas de cyberévénement.

Les recommandations sont alignées à celles de Sécurité publique Canada (Gestion des urgences et Un cadre de sécurité civile pour le Canada), mais axées sur la cybersécurité. Ainsi, en misant sur des initiatives nationales pour la mise au point et la mise en œuvre de politiques, de plan et de programmes variés, le guide de gestion des urgences de Sécurité publique Canada vise à aider les Canadiens à se protéger contre une variété de situations d'urgence et de sinistres. L'approche de Sécurité publique Canada pour la gestion des urgences est basée sur des travaux associés à quatre domaines :

- prévention et atténuation
- préparatifs d'urgence
- intervention face aux événements d'urgence
- reprise en cas de sinistre

De son côté, le cadre de Sécurité publique Canada permettra de guider le gouvernement et ses partenaires dans le but de renforcer l'évaluation des risques et d'assurer une collaboration pour prévenir et atténuer les menaces et les dangers auxquels les Canadiennes et Canadiens sont confrontés. Le cadre assurera ainsi une meilleure préparation, une meilleure intervention, ainsi qu'une reprise efficace. Basé sur le cadre de Sécurité publique, le document Stratégie de sécurité civile pour le Canada : Vers un 2030 marqué par la résilience identifie les priorités fédérales, provinciales et territoriales qui permettront de renforcer la résilience du Canada d'ici 2030. Les menaces comportent les catastrophes naturelles, comme les feux de forêt, ainsi que les catastrophes d'origine humaine, comme les déversements de matières dangereuses. Nous vous recommandons également de mettre au point des stratégies de préparation en cas d'urgence pour ces autres types de menaces.

1.1 Avantage de disposer d'un plan de préparation en cas d'urgence

Les perturbations causées par des événements imprévus peuvent avoir une incidence catastrophique sur votre organisation et sa posture de sécurité. Une préparation en cas d'urgence détaillée pourra vous aider dans les situations suivantes :

- atténuer la gravité des perturbations ainsi que les répercussions sur les activités et les services de votre organisation

- réduire le temps de reprise et assurer une restauration rapide des services
- améliorer la sécurité
- minimiser les répercussions financières des perturbations
- prévenir les dommages à la réputation
- prévenir l'application potentielle de sanctions réglementaires ou juridiques lorsqu'un plan de préparation en cas d'urgence est obligatoire
- offrir des moyens de rechange pour assurer la poursuite des opérations
- former et informer les employés au sujet des procédures d'urgence
- favoriser une meilleure identification des incidents et un déploiement rapide pour le rétablissement des services

1.2 Intervention en cas d'incident, continuité des activités et reprise après sinistre

Ces activités sont associées aux trois plans constitutifs de votre stratégie de préparation en cas de cyberurgences, soit votre PICI, votre PCA et votre PRS. Dans la présente section, nous comparerons ces trois plans et soulignerons les particularités importantes de chacun.

1.2.1 Plan d'intervention en cas d'incident

Un PICI comprend les processus, les procédures et la documentation associés aux moyens utilisés par votre organisation pour détecter, répondre et rétablir ses activités après un incident particulier. Ce plan aidera à réduire les temps d'arrêt subits par votre organisation dans l'éventualité d'un incident, ainsi que les interruptions générales des activités. Un PICI robuste traite des différents types d'incidents pouvant avoir une incidence sur votre organisation et fournit des directives étape par étape sur la façon de traiter un incident, d'atténuer les risques connexes et d'assurer une reprise rapide. Voici quelques exemples de cyberincidents qui peuvent avoir une incidence sur la posture de sécurité de votre organisation :

- rançongiciel : type de maliciel qui vous empêche d'accéder à vos fichiers ou à vos systèmes, et ce, tant que vous n'avez pas versé une rançon à l'auteur de menace. Toutefois, même en cas de paiement, vous ne bénéficiez d'aucune garantie que vous aurez à nouveau accès à vos données.
- vol de données : se produit lorsque les auteurs de menace volent de l'information stockée sur les serveurs ou les dispositifs
- exploitation active : tire avantage des logiciels et du matériel non corrigé, ou d'autres vulnérabilités connexes, afin de prendre le contrôle de vos systèmes, de vos réseaux et de vos appareils

1.2.2 Plan de continuité des activités

Un PCA est votre plan s'appliquant de manière spécifique à la reprise de vos services les plus importants, et ce, le plus rapidement possible. Il s'agit d'un plan proactif qui décrit les procédures opérationnelles qui aideront votre organisation à assurer ses activités, même en cas de perturbation. En particulier, le PCA permettra d'identifier vos actifs importants ainsi que les rôles, les responsabilités et les processus nécessaires afin d'assurer la continuité des opérations.

Votre PCA doit être basé sur votre évaluation des menaces et des risques (EMR) des technologies de l'information (TI) ainsi que sur votre analyse des répercussions sur les opérations (ARO). Votre ARO vous aidera à déterminer les impacts potentiels des interruptions dans différents scénarios de vos activités opérationnelles. Par exemple, une ARO doit répondre aux questions suivantes :

- Quelles sont les ressources et les activités critiques à la poursuite de vos activités d'affaires?
- Quelle est la durée maximale d'un arrêt éventuel de vos opérations sans que cela cause préjudice à vos activités?
- Quelles sont les répercussions financières de ces interruptions?

Une ARO présente les coûts financiers projetés associés à différentes interruptions, le cas échéant. De la sorte, vous pourrez investir de manière informée dans les stratégies de prévention et d'atténuation décrites dans votre PCA.

1.2.3 Plan de reprise après sinistre

Un PRS est un document formel qui définit un ensemble de processus et procédures ainsi que les responsabilités et les rôles particuliers des membres concernés pour le rétablissement d'une organisation à son état normal à la suite d'un événement important.

La plupart des PRS incluent une relocalisation d'emplacement physique d'infrastructures côté serveur (par exemple, déplacement des centres de données) ou encore de points d'extrémité côté client (par exemple, déménagement des bureaux), selon la portée du sinistre (inondation du centre de données ou évacuation des bureaux). Un PRS devrait également spécifier les objectifs de reprise pour tous les actifs indispensables ainsi que les étapes nécessaires afin de réduire les pertes ou les répercussions pour l'organisation.

Un PRS comprend les principes généraux d'un PICI et d'un PCA et peut fournir des conseils à propos du plan à exécuter en fonction du type d'interruption ou d'incident.

1.2.4 Différences importantes entre ces différents plans

Les PICI, les PCA et les PRS peuvent avoir beaucoup d'éléments en commun, car ils visent tous à améliorer la résilience de votre organisation, à réduire les impacts des incidents et à assurer la continuité des activités. Toutefois, il existe des différences importantes.

Un PICI est centré sur les événements et s'applique spécifiquement à un incident de sécurité, comme une cyberattaque, qui affecte une organisation. Il définit les rôles et les responsabilités et établit la portée des actions requises pour atténuer les répercussions d'un incident (par exemple, une violation de données, une attaque par rançongiciel ou une attaque par hameçonnage). Un PICI assistera votre équipe d'intervention en cas d'incident pour la réduction des périodes d'indisponibilité de l'organisation.

Un **PCA** est un plan spécifiquement adapté à la reprise rapide des opérations les plus critiques dans l'éventualité d'une catastrophe, comme définies dans l'ARO. Il établit typiquement les services devant recevoir la priorité, le personnel critique nécessaire pour l'exécution des services et un emplacement hors site à partir duquel il sera possible de mener les activités sur une base temporaire.

Un **PRS** est un plan global pour un retour aux opérations complètes de votre organisation après une catastrophe. Il traitera différents types d'interruption, comme les risques naturels, les pannes matérielles et d'alimentation, ainsi que les cyberattaques.

Chacun de ces trois plans présente les points essentiels suivants pour la réussite des activités d'identification, de gestion, d'intervention et de reprise en cas d'événement ou d'incident :

- établissement d'un point de contact désigné, d'une équipe d'intervention (ainsi que des substituts en cas de non-disponibilité), ainsi qu'une liste des rôles et des responsabilités
- programmation des vérifications périodiques afin d'identifier les lacunes potentielles ainsi que les points pouvant être améliorés
- programmation des activités de tests des plans au moyen d'interruptions simulées dans le but de s'assurer que les lacunes ont été corrigées

Une mise en œuvre de ces trois plans permettra d'améliorer votre posture de sécurité. De plus, une mise en œuvre de mesures de sécurité préventives supplémentaires, comme l'application de correctifs et la mise à niveau des actifs des TI, réduira davantage les vulnérabilités de votre organisation et favorisera un meilleur état de préparation en cas d'incident. Ces mesures de sécurité supplémentaires pourront aider votre organisation à éviter les temps d'arrêt et les interruptions des activités. En plus de mettre au point et de tenir à jour un PICI, un PCA et un PRS, nous encourageons d'améliorer votre posture de cybersécurité grâce aux moyens suivants :

- segmentation de vos réseaux afin de limiter la circulation du trafic vers les zones sensibles ou à accès restreint
- déploiement de pare-feu pour prévenir les accès au système par des sources externes non autorisées ou les déplacements de données entre différentes zones de votre réseau
- installation d'antivirus ou d'antimaliciels pour la protection de votre périmètre
- application des mises à jour et des correctifs aux systèmes d'exploitation, aux logiciels et aux micrologiciels

2 Planification des interventions en cas d'incident

Les cybermenaces peuvent avoir une incidence importante sur vos réseaux, vos systèmes et vos appareils. Grâce à un plan adéquat, vous serez prêt à gérer les incidents dès qu'ils se produisent, à atténuer les menaces et les risques connexes et à vous rétablir rapidement.

Cette section décrit les éléments préliminaires qui vous aideront à mieux créer un PICI adapté à votre organisation. Nous déterminerons les étapes principales à considérer lors de la mise au point de votre PICI et présenterons de la documentation pertinente pour vous aider à élaborer votre plan.

2.1 Points à considérer avant la création d'un plan d'intervention en cas d'incident

L'élaboration étape par étape d'un PICI peut nécessiter beaucoup de temps et sembler accablante. Bien que votre plan sera adapté à la taille de votre organisation, à vos opérations et à vos exigences de sécurité, il existe des éléments préliminaires et de base que toutes les organisations et toutes les entreprises, peu importe la taille, doivent prendre en considération :

2.1.1 Évaluation des menaces et des risques

Une EMR est un outil critique pour comprendre les différentes menaces de vos systèmes des TI, déterminer le niveau de risques auxquels ces systèmes sont exposés et recommander des protections appropriées.

Avant de créer un PICI, votre organisation doit mener une EMR. La première étape d'une EMR est l'identification des actifs critiques. Après cette identification, classez les actifs selon leur importance, leur valeur et leur niveau de risque. Cela vous permettra de créer un budget et de déterminer les outils et les ressources qui seront nécessaires pour protéger vos actifs les plus précieux.

Comme nous l'avons mentionné précédemment, il existe différents types d'incidents à considérer lors de l'élaboration d'un PICI. Votre plan doit appliquer une variété de scénarios d'intervention en cas d'incident afin de traiter chacun des types de menaces. La réalisation d'une EMR vous aidera à déterminer les risques et les menaces potentielles associés aux actifs de votre organisation, ainsi que la probabilité et les répercussions d'une compromission.

2.1.2 Création d'une équipe d'intervention

Sélectionnez les personnes qui disposent des qualifications pour participer à une équipe d'intervention et assurez-vous qu'elles comprennent leur rôle. Votre équipe doit être composée d'employés de différents domaines et bénéficier d'un soutien multifonctionnel d'autres secteurs d'activités. L'objectif principal de l'équipe d'intervention est de coordonner les ressources, de minimiser l'impact d'un incitent et d'assurer une reprise des activités aussi rapidement que possible. L'équipe d'intervention est responsable d'évaluer et de documenter les incidents, ainsi que d'y répondre. Elle est également responsable du rétablissement des systèmes, de la récupération des données et de la réduction des risques de réoccurrence d'incident.

2.1.3 Élaboration des politiques et procédures

Vos mesures d'intervention doivent cadrer avec les politiques et les exigences de conformité de votre organisation. Ainsi, votre organisation doit mettre au point une politique d'intervention en cas d'incident qui établit les autorités, les rôles et les responsabilités lors d'intervention en cas d'incident. Les membres de la haute direction et les cadres supérieures et supérieurs doivent de plus approuver cette politique. Au fil du temps, vos politiques devront être révisées et ajustées en fonction des exigences d'affaire de votre organisation.

2.1.4 Création d'un plan de communication

Votre plan de communication doit détailler la manière et le moment des communications, ainsi que les personnes à rejoindre. Il doit aussi établir qui est responsable de ces communications. Le plan de communication doit inclure un point de contact unique centralisé pour les employées et employés afin qu'ils puissent signaler les incidents, réels ou suspectés. Il doit aussi prévoir des méthodes de communication de rechange si les modes de communications courants ont été affectés par l'incident. De nombreuses organisations préfèrent nommer une seule personne désignée pour les communications avec la presse et le public en général durant une reprise après incident.

Les procédures de notification sont essentielles au succès de l'intervention en cas d'incident. Identifiez les parties prenantes internes et externes clés qui devront être avisés lors d'un incident. Il se peut que vous ayez à alerter des tierces parties, comme des clients et des fournisseurs de services gérés. Selon l'incident, il se peut également que vous ayez à communiquer avec la police ou une instance réglementaire ou que vous deviez demander conseil à une avocate ou un avocat.

Dans certains cas, vous devrez signaler l'incident au Commissariat à la protection de la vie privée du Canada (CPVP) ou à la législation pertinente en matière de confidentialité, selon votre organisation. Par exemple, si votre organisation est assujettie à *La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* du CPVP, vous devez réaliser ce qui suit :

- signaler les violations au CPVP ayant trait aux renseignements personnels posant un risque réel pour des personnes
- aviser les personnes concernées à propos des violations
- conserver un registre de toutes les violations

Le document Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité du CPVP offre une présentation de ce que vous devez connaître au sujet de ces obligations.

2.1.5 Sensibilisation du personnel

Informez les employées et employés de la planification et de l'exécution des mesures d'intervention en cas d'incident. Adaptez les programmes de formation aux besoins et aux exigences d'affaires de votre organisation, ainsi qu'aux rôles et aux responsabilités de votre personnel. Exécutez un exercice de simulation avec les employées et employés clés qui auront été identifiés dans le plan. Une bonne coopération de vos employées et employés pourra réduire votre temps d'intervention et faciliter la mise en œuvre de votre PICI. Il sera également nécessaire d'offrir de la formation aux employées et employés au sujet de l'identification et du signalement des cyberattaques, comme l'hameçonnage, les attaques par harponnage et le piratage psychologique.

2.2 Autres points à considérer pour les technologies opérationnelles

Les organisations qui gèrent des technologies opérationnelles (TO) doivent traiter et atténuer les risques associés aux incidents qui peuvent mener à des pannes non prévues et avoir une incidence à la fois sur les systèmes des TI et des TO.

Les systèmes des TO et les systèmes de contrôle industriel (SCI) peuvent ajouter de la complexité à l'environnement et imposer des contraintes uniques devant être traitées. Par exemple, plusieurs SCI peuvent être déployés sans contrôles de sécurité suffisamment robustes et être exécutés en continu, même à partir d'architectures ou de protocoles non sécurisés. Tenir à jour de l'équipement plus ancien peut être difficile, et les fournisseurs sont souvent incapables de fournir un remplacement pour le matériel et les logiciels vulnérables, ce qui peut complexifier la prévention et l'intervention face aux incidents des SCI.

Les trois publications suivantes du Centre pour la cybersécurité présentent des conseils de sécurité destinés aux organisations qui gèrent des systèmes des TO, des SCI et des infrastructures essentielles :

- Protéger vos technologies opérationnelles (ITSAP.00.051)
- Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels (ITSAP.00.050)
- Considérations en matière de sécurité pour les infrastructures essentielles (ITSAP.10.100)

Pour en apprendre davantage, lisez les conseils supplémentaires publiés par Sécurité publique Canada dans le document : Élaboration d'un plan d'intervention en cas d'incident de la technologie opérationnelle et de la technologie de l'information. Cette publication offre aux organisations qui exploitent des TO au sein de leur environnement un cadre pouvant servir à mettre au point un plan d'intervention en cas de cyberincident conjoint pour les TI et les TO. Un PICI devrait être approprié, en fonction des besoins d'affaires particuliers des organisations. Le document est une approche de référence pour élaborer un PICI et contient les facteurs particuliers à considérer en fonction de la taille, des fonctions, de l'emplacement et du secteur de votre organisation.

Lors d'une EMR sur des systèmes des TO, il est important de prendre en considération les menaces associées à ces systèmes, l'impact de leurs vulnérabilités ainsi que les types de risques pouvant mener à des interruptions pour l'environnement d'exploitation.

Voici quelques exemples de vulnérabilité des TO à prendre en considération :

- **systèmes obsolètes :** les systèmes et composants qui ne sont plus pris en charge ne seront plus mis à jour par le fabricant
- **logiciels et micrologiciels non corrigés :** les composants non corrigés présentent des vulnérabilités aux menaces connues pour les systèmes et les appareils
- **périphériques :** les appareils externes connectés peuvent être exploités afin de compromettre les systèmes et les réseaux

La conception des TO accorde typiquement la priorité à la disponibilité ainsi qu'à la répétabilité et à la fiabilité des processus, comparativement à la sécurité des données. Des systèmes ou des dispositifs de TO compromis peuvent exposer les processus essentiels à des défaillances. Une compromission des TO peut avoir les répercussions suivantes sur votre organisation :

- accidents graves et catastrophe, comme des blessures ou des décès

- équipement défectueux, interruption des processus et retard des produits livrables
- compromission de la propriété intellectuelle et de l'information sensible
- perte de revenus à cause de la perturbation des processus, des coûts de réparation et des paiements de rançon
- atteinte à la crédibilité de l'organisation
- compromission des mesures de sécurité, comme les services d'urgence

La défaillance d'un dispositif des TO peut avoir une incidence sur tout un processus industriel, sans oublier les répercussions sur la sécurité des opérateurs et du public en général. La destruction et la perte des services peuvent imposer de sérieux dommages aux systèmes, aux processus et aux infrastructures à haute valeur.

Lors de l'élaboration d'un PICI, il est important pour les organisations qui gèrent des systèmes des TO de bien comprendre les implications uniques connexes. Cela favorisera une meilleure préparation et une meilleure défense contre les interruptions et les incidents associés aux TI et aux TO. Sélectionnez une équipe d'intervention qui disposera des capacités et des ressources nécessaires pour assurer une intervention et atténuer les risques associés aux incidents des TO.

2.3 Conseils pour la création d'un plan d'intervention en cas d'incident

Cette section présente des ressources de confiance qui vous aideront à mettre au point votre PICI. Pour une introduction générale au plan d'intervention en cas d'incident, y compris les exigences préalables, ainsi qu'une présentation de son importance pour votre organisation, lisez la documentation pertinente du Centre pour la cybersécurité (Élaborer un plan d'intervention en cas d'incident [ITSAP.40.003]).

De plus, le document Cybersecurity Incident & Vulnerability Response Playbooks du Cybersecurity and Infrastructure Security Agency (en anglais seulement) présente un guide pour les interventions en cas d'incident et un autre sur les interventions face aux vulnérabilités. Ces guides offrent un ensemble de normes pour les procédures opérationnelles d'intervention et de reprise en cas d'incident ou de vulnérabilité concernant des systèmes, des données ou des réseaux.

Pour des conseils supplémentaires à propos de la gestion des incidents, consultez le document ISO 22320:2018 Sécurité et résilience – Gestion des urgences – Lignes directrices pour la gestion des incidents. Celui-ci est destiné à toutes les organisations et offre des conseils sur le traitement de tous les types d'incidents, peu importe l'envergure.

Les deux cadres d'intervention en cas d'incident les plus utilisés ont été créées par le NIST et le SANS Institute :

- Le document NIST SP 800-61: Computer Security Incident Handling Guide (PDF; en anglais seulement) offre un processus en quatre étapes pour les interventions en cas d'incident. Il est présenté comme étant un processus cyclique, avec des améliorations en continu apportées aux plans en fonction des leçons apprises pendant tout le cycle de vie des incidents. Les étapes d'intervention en cas d'incident du NIST sont les suivantes :
    - Préparation
    - Détection et analyse
    - Confinement, éradication et reprise
    - Activités après l'incident
- Le guide de traitement des incidents du SANS Institute offre un processus structuré en six étapes pour les interventions en cas d'incident. Ce processus trace les grandes lignes des bases requises pour le développement

des politiques et des normes des organisations, ainsi que les rôles et les responsabilités des membres de l'équipe d'intervention. Les six étapes du plan d'intervention en cas d'incident du guide de traitement du SANS Institute sont les suivantes :

- Préparation
- Identification
- Confinement
- Éradication
- Reprise
- Leçons apprises

La principale différence entre ces deux cadres est la combinaison des étapes de confinement, d'éradication et de reprise en une seule étape par le NIST, ces étapes étant abordées de manière séparée par le SANS Institute. La raison pour laquelle le NIST fait un tel groupement est que, selon eux, il existe un certain chevauchement des activités, qui doivent être traitées conjointement.

2.4 Étapes principales d'un plan d'intervention en cas d'incident

Disposer d'un PICI aidera votre organisation à traiter les incidents, à atténuer les menaces et les risques associés et à assurer une reprise rapide. Dans cette section, nous présentons les étapes principales d'un PICI ainsi que les actions particulières que votre organisation devra entreprendre pour développer son PICI.

2.4.1 Préparation

L'étape de préparation doit commencer avant la survenue des incidents. Cela correspond au moment où vous devez établir les bons outils et les bonnes ressources pour mettre en œuvre votre PICI. Cette phase exige des vérifications périodiques et des mises à jour afin de tenir compte des menaces émergentes. À cette étape, vous devez réaliser ce qui suit :

- Mener une EMR pour identifier vos actifs précieux qui sont critiques aux opérations d'affaires, y compris les données sensibles et exclusives.
  - Définir les incidents de sécurité les plus probables de votre organisation et anticiper les étapes détaillées de votre intervention face aux incidents.
  - Mettre en œuvre un plan de gestion des actifs des TI et les politiques connexes dans le but de faire l'inventaire et le suivi de tous les actifs et services des TI de votre organisation.
  - Tenir compte du matériel, des logiciels et des données, préciser le niveau d'importance, le modèle, le numéro de série, l'emplacement, le coût de remplacement, le fabricant et le fait que l'actif soit détenu ou associé à un abonnement avec renouvellement, comme dans le cas des logiciels infonuagiques ou des logiciels-services.
- Mettre au point et documenter vos politiques de sécurité, vos normes et vos procédures qui appuient les interventions en cas d'incident.
- Mettre au point et mettre en œuvre un plan de sauvegarde.

- Déterminer les moments où il sera pertinent de réaliser des sauvegardes complètes, différentielles ou incrémentielles.
- S'assurer que les sauvegardes sont stockées hors ligne.

- Former une équipe d'intervention et affecter des rôles et des responsabilités à chaque membre.
  - Établir une voie hiérarchique efficace, et ce, à partir du début.
  - S'assurer que les employées et employés ont une formation adéquate au sujet de leurs rôles et de leurs responsabilités.
- Définir votre plan de communication pour vous assurer que les bonnes personnes répondent à un incident.
  - Inclure des critères pour faire escalader les problèmes.
  - Déterminer comment vous comptez informer les intervenants clés et la gestion tout au long de l'incident.
- Créer et exécuter des exercices d'incident simulés pour évaluer votre PICI.
  - Affiner et mettre à jour les protocoles et les procédures.
  - S'assurer que l'équipe d'intervention comprend ses rôles et ses responsabilités.

2.4.2 Détection et analyse

Il s'agit de la phase où vous devez déterminer si votre organisation a subi une intrusion ou si un de vos systèmes a été compromis. Vous devrez analyser l'incident et en identifier le type, l'origine et l'étendue des dommages. Cela représente typiquement la phase la plus difficile du processus d'intervention en cas d'incident, mais aucun des aspects ne doit être négligé. Cette étape est préliminaire au confinement, à l'analyse et à l'éradication de la menace.

La détection des incidents peut être réalisée à partir d'outils de sécurité automatisés ou grâce à des notifications et à de l'information provenant de personnes de votre organisation, ou encore de sources externes, comme des fournisseurs et des fournisseurs de services. Vous devriez créer un système de classification qui vous aidera à orienter votre intervention à une menace en fonction de son niveau d'urgence. Cela facilitera l'isolement de vos systèmes les plus vulnérables ou de ceux les plus affectés par la menace et pourra minimiser les dommages infligés à votre organisation. Votre organisation devrait également examiner l'incident en détail afin de s'assurer qu'il s'agit en effet d'un vrai positif.

2.4.3 Confinement

Le confinement est une étape critique. L'objectif est de réduire au maximum l'impact immédiat de l'incident et de prévenir sa propagation et les dommages aux autres systèmes. Le confinement est réalisé grâce à l'isolement ou au retrait de la menace. Par exemple, en désactivant un système ou en le remplaçant complètement, en le déconnectant du réseau ou encore en désactivant certaines fonctions. Assurez-vous d'avoir un système de sauvegardes redondant. De la sorte, vos données seront protégées contre le risque de suppression permanente. Vos sauvegardes devront également vous aider à rétablir vos activités opérationnelles rapidement.

Les stratégies et les procédures de confinement pourront dépendre du type d'incident, du degré de dommage pouvant être causé par l'incident ainsi que de vos exigences opérationnelles. Les stratégies de confinement seront plus faciles à mettre en œuvre si elles ont été préétablies lors de la phase de préparation, après avoir défini le niveau de risque acceptable.

En cas de retard d'exécution du plan de confinement, les auteurs de menace auront plus de temps pour accéder et compromettre d'autres systèmes, ce qui risque de causer des dommages supplémentaires. L'étape de confinement devrait ainsi couvrir les stratégies à court et à long terme et les systèmes de secours.

Voici quelques questions qui pourront vous aider à choisir la stratégie de confinement à mettre en œuvre :

- Quels sont les dommages posés par l'incident à votre organisation?
- À quel point il est important de disposer de preuves?
- Combien de temps et quelles ressources seront nécessaires pour la mise en œuvre de la stratégie?
- Pendant combien de temps vos opérations et vos systèmes peuvent-ils être à l'arrêt?
- Quelle est l'efficacité de votre stratégie? Est-ce qu'elle offre un confinement complet ou partiel?

2.4.4 Éradication

Une fois que l'incident aura été confiné, vous devrez mener une analyse de la cause profonde pour identifier et retirer tous les éléments de l'incident des systèmes affectés afin de prévenir toute compromission ultérieure. La phase d'éradication améliorera vos stratégies de défense grâce aux leçons apprises. Dans cette phase, vous devez réaliser les activités suivantes :

- identifier les systèmes, les hôtes et les services concernés
- supprimer tout contenu malveillant des systèmes affectés
- analyser et effacer les systèmes et les dispositifs infectés afin de prévenir les risques de réinfections
- identifier et traiter les vecteurs d'attaque résiduels pour vous assurer que les autres systèmes ne sont pas compromis
- communiquer avec l'ensemble des parties prenantes afin de vous assurer d'une gestion adéquate de l'incident
- renforcer, corriger et mettre à niveau les systèmes concernés
- mettre à niveau ou remplacer les systèmes patrimoniaux

2.4.5 Reprise

À la phase de reprise, vous devrez restaurer et réintégrer les systèmes affectés dans votre environnement d'exploitation. Afin d'éviter les réinfections après un cyberincident, adoptez certaines mesures préventives, comme vous assurer que les maliciels ont été supprimés avant la restauration des sauvegardes. Vous devrez de plus tester, vérifier, surveiller et valider les systèmes affectés pour vous assurer qu'ils fonctionnent adéquatement. Votre organisation devra aussi réviser et mettre à jour ses politiques, ses procédures et ses initiatives de formation.

Lors de cette étape, aidez-vous de questions suivantes :

- À quel moment les systèmes pourront-ils être réintégrés dans l'environnement opérationnel?
- Pendant combien de temps devrez-vous surveiller les systèmes afin de détecter tout comportement anormal?
- Comment procéderez-vous pour tester les systèmes compromis pour vous assurer qu'ils ne présentent plus une menace?

- Quels outils peuvent vous aider à éviter des attaques similaires à l'avenir?

2.4.6 Activités post-incidentes et leçons apprises

L'objectif de cette étape est d'analyser et de documenter tout ce que vous connaissez de l'incident. Il est important de créer des rapports de suivi, qui présenteront une évaluation de ce qui est arrivé tout au long du processus de traitement des incidents. Le rapport servira d'outil pour renforcer la résilience de votre organisation en identifiant les façons d'améliorer vos efforts d'intervention, vos mesures de sécurité et vos composants associés au processus de traitement des incidents.

Dans le but de faciliter la collecte de l'information pertinente au rapport, tenez une réunion rassemblant tous les membres ayant participé à l'intervention peu de temps après la reprise afin de discuter des points importants. Par exemple :

- À quel moment l'incident est-il survenu? Pourquoi? Quel a été l'élément déclencheur?
- Est-ce que l'équipe d'intervention a été efficace? Est-ce que les rôles et les responsabilités étaient bien établis?
- Est-ce que l'équipe d'incident doit modifier son plan d'action pour les incidents à venir?
- Est-ce que les procédures documentées ont été respectées et est-ce qu'elles ont permis de traiter efficacement l'incident?
- Est-ce qu'il y a des éléments qui ont retardé ou nui au processus de reprise?
- Quelle information ou quel plan d'action aurait eu avantage à être connu plus tôt?
- Est-ce qu'il aurait été possible d'améliorer les communications et l'échange d'information avec les tierces parties? Comment?
- Est-ce que des améliorations peuvent être apportées à la formation?

3 Plan de continuité des activités

Un PCA est souvent considéré comme étant un sous-ensemble d'un PRS. Il s'agit d'un document formel contenant des directives détaillées au sujet de ce que votre organisation doit faire pour reprendre rapidement ses activités à la suite d'une catastrophe non planifiée. Seuls les services critiques sont inclus dans le PCA. Les fonctions non critiques pourront être considérées après une résolution complète de l'incident.

Le document Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences (ISO 22301) présente un cadre pour aider les organisations à planifier, à mettre en œuvre et à tenir à jour un plan de continuité des activités. Ainsi, le document ISO 22301 aidera les organisations de toutes tailles à répondre à différents types d'interruptions et à poursuivre ou à reprendre les activités par la suite.

La publication NIST SP 800-34 Revision 1 Contingency Planning Guide for Federal Information Systems (en anglais seulement) offre des directives aux agences fédéral américaines afin d'évaluer les systèmes d'information et les opérations connexes afin de déterminer les exigences et les priorités d'une planification d'urgence. La publication traite des PICI, des PCA et des PRS et peut servir de référence afin d'aider les organisations à mettre au point leurs stratégies et leurs procédures de reprise.

3.1 Perturbations principales pouvant affecter votre organisation

Bien que votre PCA doit tenir compte de tous les types d'incidents, les menaces suivantes sont celles typiques pouvant perturber vos activités :

- risques naturels, comme les ouragans, les tornades, les tremblements de terre, les inondations, les feux de forêt et les tempêtes violentes
- incendies d'un bâtiment
- cybermenaces, comme les attaques par rançongiciel, les vols de données et les attaques par déni de service distribué
- pannes de serveur ou des services publics, comme les pannes de courant, les pannes de communication ou les coupures d'eau
- défaillance d'équipement pouvant avoir une incidence sur les opérations, comme les systèmes de chauffage, de ventilation et de conditionnement d'air, l'équipement de bureau ou l'équipement de fabrication
- actes terroristes
- pandémie mondiale, comme une épidémie ou une urgence de santé publique liée à un virus
- problème de fabrication ou de distribution en raison d'une interruption de la chaîne d'approvisionnement

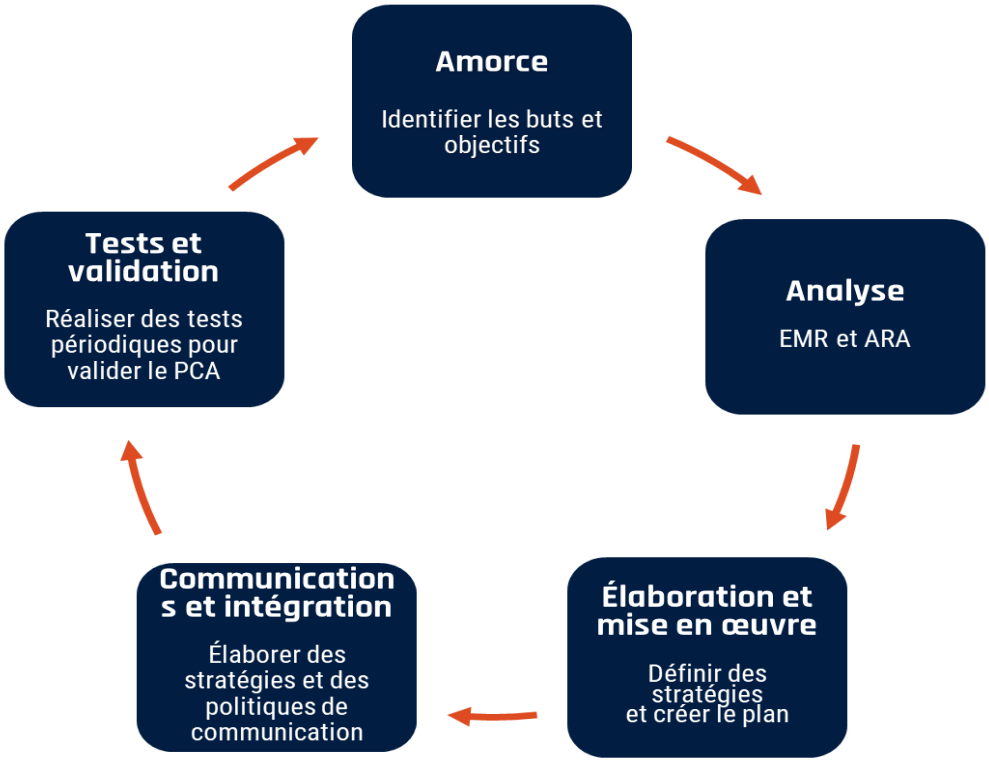
3.2 Étapes pour l'élaboration de votre plan de continuité des activités

Dans cette section, nous discuterons des points particuliers dont votre organisation devra tenir compte lors de l'élaboration de votre PCA pour en assurer l'efficacité. Un PCA permet aux organisations d'identifier les risques provenant d'une variété de menaces ainsi que leur incidence sur les activités d'affaires. Un PCA favorise la résilience de votre organisation, ainsi que

la conformité aux réglementations, aux politiques et aux normes. L'objectif d'un PCA est d'identifier toutes les ressources et procédures nécessaires afin que les organisations puissent poursuivre leurs opérations critiques dans l'éventualité d'une catastrophe ou de tout autre type de perturbation.

La planification de la continuité des activités est une approche échelonnée et exige des évaluations, des tests et des mises à jour en continu. Voir l'image ci-dessous, figure 1 : Le cycle de planification de la continuité des activités est composé de cinq étapes importantes pour l'élaboration et la mise à jour d'un PCA.

Figure 1: Cycle de vie du plan de continuité des activités



Description longue : Figure 1 : Cycle de planification de la continuité des activités décrivant les cinq étapes du cycle de vie de la planification de la continuité des activités.

- Amorce : Identifiez les buts et objectifs uniques de votre organisation.
- Analyse : Menez une EMR et une ARO
- Élaboration et mise en œuvre : Définissez la stratégie, mettez au point un plan et mettez-le en œuvre.
- Communications et intégration : Communiquez votre PCA à vos employés, à vos intervenants et à vos partenaires et intégrez-le à vos politiques organisationnelles.
- Tests et validation : Testez votre plan périodiquement pour vous assurer de son efficacité et de sa pertinence.

La section suivante décrit les cinq étapes du cycle de vie du plan de continuité des activités.

3.2.1 Amorce : Identification des buts, des objectifs et de la réponse de votre plan

L'objectif principal d'un PCA est de s'assurer que les fonctions d'affaires critiques subiront une interruption minimale dans l'éventualité d'une catastrophe ou d'un incident. Toutefois, selon les exigences uniques et les ressources de votre organisation, il se peut que vous ayez des objectifs ou des buts différents. Après avoir déterminé vos objectifs et vos buts, assurez-vous de les communiquer clairement. De plus, ils doivent être bien acceptés par la haute direction de votre organisation. Vos objectifs influenceront votre EMR, votre ARO, votre PCA et vos stratégies de reprise.

Vous devrez déterminer les personnes et les processus clés pour assurer l'atteindre de vos objectifs. Vous devrez également disposer d'un plan de communications adapté. Établissez une équipe de gestion constituée de personnes qui connaissent les différents secteurs opérationnels de votre organisation afin d'évaluer le potentiel des menaces pouvant mener à différents risques pour votre organisation. La création de votre équipe pourra dépendre de vos objectifs de continuité des activités et de la taille de votre organisation. En outre, vous devrez affecter un chef d'équipe qui pourra assurer la réalisation de l'élaboration, de la mise en œuvre, des modifications et des mises à jour de votre plan.

3.2.2 Analyse : Réalisation des évaluations requises

Après avoir déterminé vos buts et objectifs, vous devez mener une EMR détaillée. Il est important que votre organisation comprenne bien où se trouvent les risques ainsi que les différentes menaces pouvant perturber vos opérations d'affaires. Cette compréhension vous aidera à déterminer comment réduire, atténuer et éliminer les risques sous-jacents.

Une fois que votre organisation aura déterminé les menaces potentielles, il sera nécessaire de réaliser une ARO pour identifier les opérations et les systèmes d'affaires critiques et non critiques ainsi que les répercussions de différentes menaces dans différents secteurs de vos activités. Une ARO déterminera les menaces particulières qui pourront avoir une incidence financière ainsi que sur les performances opérationnelles, les employés, les chaînes d'approvisionnement, les ressources et la réputation de votre organisation. Il sera nécessaire d'analyser ces menaces afin de déterminer leur probabilité de survenue ainsi que le niveau de gravité associé. Les stratégies d'atténuation qui peuvent réduire la probabilité de survenue ainsi que le niveau de gravité doivent également être identifiées.

La collaboration est la clé lors d'une ARO. Les gestionnaires, les principaux intervenants, les partenaires et les employés doivent tous être intégrés aux discussions. Cela vous fournira une meilleure vue d'ensemble au sujet des répercussions des catastrophes sur les activités des autres fonctions de votre organisation. Par ailleurs, les intervenants et les partenaires seront ainsi mieux en mesure de comprendre leurs propres risques sur leurs opérations d'affaires et de déterminer des stratégies d'atténuations de ces risques.

Documentez tous les résultats de votre EMR et de votre ARO. De la sorte, vous pourrez anticiper les coûts et les ressources qui seront nécessaires pour une reprise après un sinistre ou un incident.

Pour faciliter vos activités d'EMR et d'ARO, nous vous suggérons de catégoriser la sécurité de vos activités opérationnelles (par exemple, les processus opérationnels et les renseignements à propos de l'information connexe). Cette catégorisation vous aidera à établir l'importance relative de vos activités opérationnelles. Au niveau du système d'information, la catégorisation de la sécurité des activités opérationnelles sert de données d'entrée pour établir les exigences d'assurance de sécurité, sélectionner et adapter les contrôles de sécurité et mener une EMR. La catégorisation de la sécurité est un processus permettant de déterminer les répercussions pouvant découler des compromissions ainsi que leur niveau de gravité, en fonction des objectifs de sécurité, de confidentialité, d'intégrité et de disponibilité. Le résultat de ce processus

pour une activité opérationnelle est la catégorie de sécurité exprimant le plus haut niveau de répercussion attendu, en fonction des trois objectifs de sécurité des TI. Pour obtenir de plus amples renseignements et des conseils à propos de la catégorisation de la sécurité, lisez le document La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) du Centre pour la cybersécurité.

3.2.3 Élaboration et mise en œuvre : Définition de la stratégie et création du plan

Une fois que vous aurez identifié les types de risque, les menaces et les vulnérabilités qui s'appliquent à votre organisation, vous pourrez commencer à mettre au point un PCA efficace. Votre plan devrait porter sur les stratégies d'atténuation des risques qui ont été déterminés. De la sorte, vous serez mieux en mesure d'assurer une reprise de vos activités essentielles. Un PCA complet prendra en considération chaque risque qui aura été identifié dans l'ARO ainsi qu'une stratégie d'intervention appropriée afin d'en minimiser les répercussions pour les parties prenantes, les opérations et les actifs de votre organisation, ou sinon les atténuer le plus possible. Voici quelques pratiques exemplaires à prendre en considération lors de l'élaboration de votre PCA :

- détermination des membres de l'équipe d'intervention et description détaillée des rôles et des responsabilités afin que les personnes puissent réagir rapidement et efficacement
- moyens de communication et procédures de reprise
- lieu de travail de rechange et plan de déménagement des employées et employés
- liste consolidée des ressources et des fournisseurs de rechange
- plan de reprise informatique, cohérent à la publication Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004) du Centre pour la cybersécurité
- politiques à mettre en pratique durant une catastrophe, une urgence ou un incident
- budget nécessaire pour les différentes activités de votre plan
- période pendant laquelle les services et les activités opérationnelles devront être disponibles
- ressources nécessaires pour assurer les niveaux de priorité établis et une intervention rapide et adaptée
- création de rapports à partager avec les intervenants
- formation et sensibilisation du personnel à propos des risques variés et des différentes stratégies de préparation et d'intervention en cas d'urgence
- documentation, validation du plan et partage de ce dernier avec la gestion et la haute direction dans le but d'obtenir une approbation
- stockage du document du PCA dans un emplacement sécurisé et accessible en cas de besoin

3.2.4 Communications et intégration : Élaboration des politiques et des protocoles de communication

Une fois que vous aurez créé votre PCA, transmettez-le à vos employées et employés, à vos parties prenantes et à vos partenaires et intégrez-le à vos politiques organisationnelles. Celui-ci devrait être facilement accessible afin de permettre à l'équipe d'intervention de bien coordonner ses efforts. Vous devriez également mettre au point des plans détaillés pour les

communications et les relations publiques, notamment concernant les communications avec le personnel, les investisseurs et les médias. De la sorte, vous serez mieux en mesure d'éviter la propagation de mésinformation.

Votre PCA doit inclure des stratégies de communication efficaces, à la fois pour les membres internes et les parties prenantes externes. Des communications claires au sein de votre organisation durant une crise permettront de rassurer vos employées et employés en précisant que vous avez entrepris les étapes pour assurer une intervention et une reprise rapides. Les communications avec les parties prenantes externes, les fournisseurs et les clientes et clients sont également primordiales pour minimiser les dommages à la réputation et maintenir l'intégrité de votre organisation.

Le processus de communication devrait inclure des protocoles et des procédures permettant de choisir les mesures de protection appropriées et d'aviser les bonnes personnes. Des messages prérédigés faciliteront et accéléreront vos communications dans l'éventualité d'une crise.

3.2.5 Tests et validation : Tests périodiques pour la validation de votre plan

Les risques de votre organisation ne sont pas statiques et pourraient bien changer au fil du temps. Vos activités d'affaires et vos priorités peuvent également évoluer. De la sorte, votre PCA devra être réévalué et testé périodiquement afin d'assurer qu'il restera efficace et à jour. Un PCA robuste peut être amélioré au moyen d'analyses continues, de tests et des activités de validation et de mise en œuvre. Vous devrez mener des exercices de simulations et réels pour évaluer l'état de préparation de votre équipe d'intervention ainsi que les points faibles de votre plan. Vous pouvez choisir différents types d'exercice pour tester votre plan, comme des séminaires, des exercices de simulation et des exercices réels. N'oubliez pas d'exploiter les leçons apprises de vos exercices et de vos tests afin de mettre à jour votre PCA. Une liste de vérification permettra d'assurer que chaque partie de votre pan fonctionne adéquatement et qu'elle mène à des résultats bénéfiques.

Les pratiques de test de PCA doivent inclure ce qui suit :

- Évaluation de la sensibilisation, de la formation et des protocoles. Par exemple, en vous assurant que les protocoles sont pertinents et en offrant des séances de formation périodiques aux employées et employés et aux membres de l'équipe d'intervention.
- Tests, évaluation et validation des solutions techniques et des étapes qui figurent dans le PCA. Par exemple, en vous assurant que les solutions et les étapes sont toujours efficaces. Vous devrez les mettre à jour, au besoin.
- Tests, évaluations et validation des procédures de reprise établies dans le PCA. Par exemple, en vous assurant que les procédures restent alignées aux exigences opérationnelles et au paysage de menaces de votre organisation.

4 Plan de reprise après sinistre

Un PRS examine chaque aspect de votre organisation pouvant être affecté, comme les actifs, l'infrastructure, les ressources humaines et les partenaires commerciaux. Dans votre PRS, vous devriez déterminer les activités opérationnelles critiques et non critiques. Cela devrait comprendre les exigences, les procédures et les instructions détaillées pour chaque fonction critique. De la sorte, vous serez mieux en mesure de protéger les actifs et les activités opérationnelles de votre organisation afin de répondre à vos exigences opérationnelles et de limiter au minimum les temps d'arrêt.

Le PRS devrait définir des stratégies pour réduire l'impact d'une catastrophe et rétablir les actifs et les services des TI aussi rapidement que possible afin d'assurer la continuité des opérations critiques.

Un sinistre, peu importe sa nature, peut avoir des répercussions dévastatrices sur votre organisation. Plus le temps de reprise sera long, plus les dommages risquent d'être importants. De la sorte, il est important de disposer d'un bon PRS qui assurera une reprise rapide, peu importe le type de catastrophe.

Un PRS doit être organisé selon le type de catastrophe et l'emplacement. De plus, il doit fournir des instructions étape par étape pour une mise en œuvre facile.

La publication du Centre pour la cybersécurité, Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004), présente les éléments importants ainsi que les étapes qui peuvent vous aider à mettre au point un PRS. Elle décrit également comment un plan de reprise peut améliorer la résilience générale ainsi que la posture de cybersécurité de votre organisation. La consultation d'autres ressources pour élaborer votre PRS, comme les documents rédigés par IBM Disaster recovery plan template ou Cybersécurité — Préparation des technologies de l'information et de la communication pour la continuité d'activité peut également être utile.

Dans la prochaine section, nous décrirons les éléments importants d'un PRS. Comme nous l'avons mentionné précédemment, un PICI et un PRS présentent certaines similarités. Bien que des points se répètent dans la prochaine section, il est important de rappeler ces éléments clés, car ils permettent de donner forme au PRS.

4.1 Éléments importants d'un plan de reprise après sinistre

Dans cette section, nous discuterons des aspects particuliers que votre organisation devra traiter lors de l'élaboration d'un PRS. Ces étapes permettront un retour aux opérations complètes de votre organisation après une catastrophe.

4.1.1 Création d'une équipe de reprise après sinistre

L'objectif de l'équipe de reprise après sinistre est d'assurer la reprise des systèmes, la récupération de l'information et la réduction des risques de nouvelle survenue de l'incident. Le plan devrait clairement identifier le nom et les coordonnées des personnes responsables des différents aspects du processus de reprise après sinistre. Cela facilitera les communications lorsque les efforts de reprise seront en cours.

Les membres de l'équipe devraient être adéquatement formés sur le sujet de la reprise après sinistre et devraient comprendre leurs rôles et leurs responsabilités. L'équipe doit être composée d'employés de différents domaines et bénéficier d'un soutien multifonctionnel d'autres secteurs d'activités. Puisque les incidents sont impossibles à prévoir et qu'ils exigent une intervention immédiate, pensez également à créer une équipe d'intervenantes et intervenants d'urgence

pour assurer une présence même en cas d'absence des personnes en cas d'incident. Les responsabilités critiques sont les suivantes :

- identification d'un responsable du plan, qui dirigera le processus de reprise avec l'appui de la haute direction et des gestionnaires de l'organisation
- création d'un plan de communications qui traite des points importants afin de transmettre l'information essentielle aux principales parties prenantes et aux médias
- mise en œuvre et tenue à jour d'un système de sauvegarde pour assurer la continuité des activités

4.1.2 Tenue à jour d'un inventaire de tous vos actifs des TI et identification des éléments les plus essentiels

Pour disposer d'un PRS efficace, vous devez maintenir un inventaire à jour de vos actifs des TI. Votre inventaire devrait inclure une liste du matériel, des logiciels et des actifs informationnels, en plus d'en préciser l'emplacement. Vos actifs devraient être catégorisés en fonction de leur criticité pour vos opérations. Vos actifs les plus critiques incluent les données sensibles et exclusives, ainsi que les actifs qui sont essentiels à vos activités d'affaires. La criticité devrait être comparée aux probabilités de risque et au niveau de résilience des actifs en situation de sinistre. Cela vous permettra de mieux anticiper et de gérer les risques.

Votre organisation doit classer ses actifs, du plus critique au moins critique, afin de définir la portée de son PRS. Assurez-vous que votre PRS permet de traiter les actifs critiques à haut risque en premier, y compris vos données sensibles. Les données sensibles peuvent être sujettes à des exigences de conformité, comme la *Loi sur la protection des renseignements personnels du Canada (LPRP)*, ou encore la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), qui couvre le traitement des renseignements personnels des organisations du secteur privé. Votre PRS devrait identifier comment vos données sensibles seront protégées et sauvegardées de manière sécurisée.

4.1.3 Tolérance au risque de votre organisation

Pour mieux appuyer vos efforts de gestion du risque et de reprise, vous devez déterminer et documenter les risques de votre organisation, ainsi que votre niveau de tolérance vis-à-vis de ces risques. Par la suite, votre organisation sera mieux outillée pour établir ses stratégies de reprise, et ce, en fonction d'une variété de sinistres. Votre PRS devrait inclure différents événements, comme des risques naturels, des pannes de courant, des cyberattaques, des attaques de rançongiciel, des menaces internes et des défaillances d'équipement critique.

Voici quelques points importants pour vous aider à identifier votre tolérance à l'égard des risques :

- activités opérationnelles critiques
- activités opérationnelles qui traitent des données sensibles
- actifs qui ont de la valeur pour votre organisation, y compris les données
- particularités de votre emplacement et de votre infrastructure; cela pourra vous aider à déterminer si vous avez besoin d'une sauvegarde infonuagique, d'un ou de plusieurs sites de stockages et de serveurs de rechange

4.1.4 Identification des opérations critiques

Votre PRS doit identifier quelles sont les activités opérationnelles qui sont considérées comme critiques pour votre organisation. Pour mieux déterminer vos opérations critiques, posez-vous les questions suivantes :

- Quels composants de vos activités sont importants pour assurer la survie de votre organisation si un accès immédiat n'est plus possible?
- Quels sont les données ou les renseignements stockés qui, en cas de perte, pourraient engendrer des répercussions juridiques ou nuire à votre réputation?
- Quels sont les brevets, les propriétés intellectuelles ou les renseignements commerciaux nécessaires pour protéger et assurer votre réputation dans l'industrie et pour protéger vos activités?

En comprenant bien les ressources qui ont le plus de valeur pour votre organisation, vous serez mieux équipé pour mettre en œuvre des stratégies dans votre PRS pour assurer votre résilience dans une situation de catastrophe.

4.1.5 Élaboration de procédures de reprise après sinistre

Les procédures documentées de reprise étape par étape sont un composant majeur d'un PRS. Ces procédures décrivent l'intervention de votre organisation face à différents sinistres. En situation d'événement catastrophique inattendu, votre organisation disposera de très peu de temps pour réagir. Disposer de procédures de reprise après sinistre permettra à votre équipe d'intervention de savoir exactement ce qu'il faut faire pour minimiser les dommages et éviter les pannes prolongées. Ces procédures devraient, au minimum, traiter les points suivants :

- **procédures d'intervention en cas d'urgence**, qui incluent les étapes nécessaires afin de répondre efficacement aux situations d'urgence, de minimiser les dommages et de protéger vos employés
- **procédures de sauvegarde pour les opérations d'affaires**, qui assureront des interruptions minimales des activités opérationnelles essentielles de votre organisation
- **procédures pour déterminer les actions de reprise après sinistre**, qui aideront à rétablir votre environnement d'exploitation, y compris les systèmes, les réseaux, les appareils et l'accès aux données et aux renseignements à la suite d'un sinistre

4.1.6 Identification des objectifs de délai de rétablissement et des objectifs de point de rétablissement

Les objectifs de délai de rétablissement (ODR) et les objectifs de point de rétablissement (OPR) sont des mesures servant à déterminer votre tolérance aux périodes d'indisponibilité et aux pertes de données respectivement.

L'ODR est la période d'indisponibilité maximale préétablie que votre organisation pourra tolérer sans que cela occasionne de préjudices. Celle-ci peut être mesurée en minutes, en heures, en jours ou en semaines. L'ODR est le temps prévu et le niveau de service nécessaires pour répondre aux attentes minimales du propriétaire du système.

Pensez à créer différentes catégories d'ODR, car certaines activités opérationnelles nécessiteront des délais de reprise plus courts, comparativement à d'autres secteurs moins critiques pour la survie de votre organisation. Voici quelques facteurs importants à considérer lors de l'établissement des ODR :

- analyse coûts-avantages associée au rétablissement de vos opérations
- coûts pour l'atténuation
- niveau de complexité du processus de reprise
- temps et ressources nécessaires pour retourner à une situation opérationnelle normale
- classement et niveau de priorité des actifs indispensables servant à une reprise stratégique

L'OPR est la perte maximale de données que votre organisation peut tolérer avant que cela n'occasionne des répercussions négatives. L'OPR est mesuré en unité de temps. Il s'agit essentiellement de la période entre le début de la panne et votre dernière sauvegarde valide des données.

Pour certaines organisations, le roulement des données peut être faible, et un OPR se mesurant en jours, ou même en semaines, peut être tolérable. Pour les organisations associées à un haut débit de transactions de données, il peut être inadmissible de perdre les données des dernières heures, ou même des dernières minutes. L'OPR peut servir de mesure pour bien comprendre la fréquence et les emplacements de sauvegarde des données ainsi que l'importance de ces données pour de votre organisation. Certaines bases de données transactionnelles peuvent être configurées pour une copie synchrone vers les sites de reprise après sinistre. Cela permet d'assurer qu'aucune donnée n'est perdue, mais la vitesse des transactions peut être affectée sensiblement, et les coûts peuvent également être plus importants.

Lors de l'établissement de l'impact sur les activités d'une catastrophe, la somme des mesures OPR (à partir de la catastrophe) et ODR (à la suite de la catastrophe) permet de donner une idée des pertes des activités considérées dans le PRS. Les mesures ODR et OPR doivent être évaluées et mises à jour régulièrement, car elles peuvent vraisemblablement changer en fonction du paysage des menaces et des changements de vos objectifs et de vos opérations d'affaires.

4.1.7 Établissement d'un site de reprise après sinistre

Un PRS doit indiquer où les actifs de votre organisation se trouvent en cas de sinistre. Les sites de reprise sont généralement associés à un emplacement distant. Ils servent à faciliter la reprise de l'infrastructure des TI et d'autres opérations essentielles à l'organisation durant un incident.

Il est important de documenter les différentes caractéristiques des installations physiques concernées, y compris l'emplacement, le chauffage, la climatisation, l'alimentation, la prévention des incendies et les contrôles de sécurité.

L'établissement d'un site de reprise après sinistre peut être dispendieux. Si votre organisation ne dispose pas des ressources financières pour avoir son propre site de reprise, il peut être intéressant d'avoir recours à un fournisseur de services qui pourra héberger votre infrastructure distante, fournir un PRS à partir du nuage ou encore offrir une reprise après sinistre à titre de service (DRaaS). Nous discuterons plus en détail de ces options dans la prochaine section.

Trois choix de sites de reprise après sinistre s'offrent à vous, selon vos priorités d'affaires.

4.1.7.1 Site branché

Un site branché est un site de secours entièrement fonctionnel doté de la même infrastructure des TI que le site principal. Ses fonctions sont identiques au site principal et il est exécuté en continu pour assurer un relais en cas de panne. La synchronisation des données s'effectue également en continu afin de réduire le risque de perte de donnée. L'avantage d'un site branché est que celui-ci peut pratiquement éliminer les problèmes de temps d'arrêt.

4.1.7.2 Site chaud

Un site chaud est un site de secours présentant une connectivité réseau et quelques éléments d'équipement installés. Un site chaud exige un temps de configuration avant un fonctionnement à plein régime. La synchronisation des données survient moins souvent, ce qui peut ainsi mener à certaines pertes de données.

4.1.7.3 Salle blanche

Une salle blanche sert à stocker les systèmes de secours et les sauvegardes de données, mais elle n'exige que peu d'équipement installé. Celle-ci nécessite plus de temps et de ressources pour la configuration et le rétablissement des activités opérationnelles. La synchronisation des données peut être difficile et longue, car les serveurs doivent être migrés de votre site principal, ce qui peut mener à des risques plus élevés de perte de données.

4.1.8 Tests et entretien d'un plan de reprise après sinistre

Votre organisation doit tester son PRS périodiquement afin de s'assurer que les procédures documentées sont efficaces et à jour. Un PRS est un processus continu qui doit être vérifié périodiquement dans le but d'assurer un bon alignement, en particulier en cas de changement des risques environnementaux, des activités opérationnelles ou des technologies utilisées.

En testant votre PRS régulièrement, vous pourrez vous assurer d'atteindre votre objectif d'intervention grâce à l'identification des points qui doivent être améliorés. En mettant à l'épreuve votre plan, vous pourrez vous assurer de ce qui suit :

- vérifier l'efficacité de la documentation au sujet de la reprise et des sites concernés
- réaffirmer que votre organisation sera en mesure de résister à un sinistre
- vous assurer que vos données sont répliquées correctement et qu'elles pourront être rétablies facilement à partir de vos sauvegardes
- évaluer les leçons apprises des incidents antérieurs et inclure de nouvelles activités d'atténuation dans votre PRS
- indiquer les points de votre PRS devant être mis à jour
- mettre à jour les exigences de formation pour votre équipe d'intervention afin de vous assurer que celle-ci est informée des changements et qu'elle est bien préparée pour la mise en œuvre de votre PRS

Il existe différents types de tests que vous pouvez utiliser pour votre PRS :

4.1.8.1 Liste de vérification

Un test au moyen d'une liste de vérification permettra de vous assurer que vos procédures de reprise sont complètes et qu'elles tiennent compte de toutes les ressources et des membres de l'équipe d'intervention jugés nécessaires pour l'exécution de chaque étape du plan.

4.1.8.2 Exercice de simulation

L'objectif principal d'un exercice de simulation est de vérifier que votre équipe d'intervention comprend les processus et les procédures de votre PRS et que les responsabilités et les rôles sont clairs. Un exercice de simulation permettra à tous les membres de l'équipe d'intervention de se coordonner et de discuter dans le cadre d'une interruption simulée. Les membres pourront discuter des actions requises pour la gestion des fins détails associés au sinistre, y compris les conséquences.

Cela permettra d'assurer de disposer des ressources nécessaires, comme indiqué dans le PRS. Un exercice de simulation pourra également déterminer si votre PRS est efficace et dévoilera ses forces et ses faiblesses, ce qui vous permettra de traiter tout problème associé à votre PRS avant la survenue réelle d'un événement.

4.1.8.3 Tests de parcours

Un test de parcours est un essai à blanc qui vous aidera à anticiper les problèmes. Il s'agit en fait d'une vérification étape par étape de votre PRS dans le but d'établir que les membres de votre équipe d'intervention comprennent bien leurs rôles, connaissent toutes les étapes du plan et qu'ils sont au courant de tous les changements apportés au plan depuis sa dernière évaluation.

4.1.8.4 Tests parallèles

Un test parallèle s'applique lorsque le système de reprise sert à restaurer un système, sans interrompre les activités d'affaires. Il s'agit d'une vérification étape par étape de chaque composant du plan pour identifier les lacunes, les faiblesses ou les détails négligés qui peuvent présenter des obstacles durant une exécution réelle.

4.1.8.5 Tests d'interruption totale

Un test d'interruption totale représente le type de test le plus rigoureux. Dans un tel cas, le système principal est mis hors service et l'équipe d'intervention tentera de le rétablir. C'est un test minutieux et long. Il est également risqué, car il peut mener à une interruption des activités et mener à un coûteux temps d'arrêt. Dans certains cas, ce type de test n'est pas envisageable en raison des questions réglementaires et associées à la sécurité publique.

4.1.8.6 Test de simulation

Un test de simulation aidera votre équipe d'intervention à savoir quoi faire en cas de sinistre. Il fait intervenir un jeu de rôle en fonction d'un scénario de catastrophe particulier dans le but de mettre votre PRS à l'épreuve. Il devrait intégrer toutes les étapes d'un PRS et permettre de s'assurer que toutes les procédures documentées sont claires et sans ambiguïtés.

4.2 Types de stratégies de reprise après sinistre

À la section précédente, nous avons discuté de la configuration de sites de reprise après sinistre afin d'aider votre organisation à protéger son infrastructure des TI et ses activités essentielles. Nous avons énuméré trois types de sites de reprise après sinistre (site branché, site chaud, salle blanche) afin de vous aider à faire votre choix, en fonction de vos priorités d'affaires, de vos ressources et de votre tolérance au risque. En plus de ces options, il existe également d'autres stratégies de reprise après sinistre à évaluer, qui peuvent dépendre de votre infrastructure des TI, de vos activités, de vos ressources, de votre budget et de vos actifs indispensables. Voici quelques exemples de méthodes de sauvegarde et de reprise de rechange à explorer.

4.2.1 Reprise après sinistre pour le réseau

La connectivité réseau est essentielle aux communications internes et externes de votre organisation, à l'accès aux applications et au partage des données. Dans l'éventualité d'une panne réseau, les procédures de reprise après sinistre pour

le réseau spécifieront comment les services réseau seront rétablis, ainsi que les ressources requises, l'accès aux données de sauvegarde et aux sites de stockage. En fonction des exigences de votre organisation, votre stratégie de reprise après sinistre pour le réseau peut inclure les éléments suivants :

- réseaux locaux (LAN)
- réseaux étendus (WAN)
- réseaux sans fil
- applications et services réseau
- défaillances d'appareil pouvant mener à une interruption de la connectivité réseau, comme les routeurs, les commutateurs, les passerelles et les modems

Il existe de nombreuses raisons pouvant mener à une interruption de la connectivité réseau, y compris une erreur humaine, des catastrophes naturelles et physiques et des cyberattaques, comme des attaques par déni de service distribué.

4.2.2 Reprise après sinistre virtuelle

Votre organisation peut utiliser des machines virtuelles qui se trouvent dans un emplacement hors site ou dans le nuage afin d'assurer une sauvegarde des opérations ou des données particulières, ou même de répliquer l'ensemble de votre infrastructure des TI (serveurs, stockage, systèmes d'exploitation, logiciels, applications et données). L'utilisation de la visualisation comme stratégie de reprise après sinistre offre un certain nombre d'avantages :

- automatisation de certains processus de reprise après sinistre et rétablissement rapide des opérations en ligne
- réduction de l'empreinte des TI
- possibilités de réplications fréquentes et de basculement transparent
- infrastructure pouvant fonctionner à partir de n'importe quel emplacement

4.2.3 Reprise après sinistre infonuagique

Une reprise après sinistre infonuagique offre des services et des stratégies pour la restauration des données de sauvegarde, des applications et d'autres ressources, et ce, à partir d'un stockage en nuage, plutôt qu'un emplacement physique. Une reprise après sinistre infonuagique peut représenter plus qu'une solution de secours en fournissant des possibilités de basculement automatique des charges de travail vers une plateforme infonuagique. De la sorte, les organisations pourront restaurer leurs sauvegardes, que ce soit dans un environnement sur place ou dans le nuage. Une telle solution permettra d'assurer la continuité des activités et une reprise rapide en cas d'interruption.

Une reprise après sinistre infonuagique facilite l'automatisation de nombreux processus de reprise et peut être gérée par niveaux afin de répondre aux exigences d'affaires. Cela est souvent offert à titre de solution logiciel-service. Il peut s'agir d'une option plus abordable pour les organisations disposant de ressources financières limitées.

Exploiter une stratégie de reprise après sinistre infonuagique offre les avantages supplémentaires suivants :

- modèle de tarification flexible, comme un paiement à la demande ou à l'utilisation
- absence de point de défaillance unique lors du recours au nuage, car vous pouvez choisir l'option de sauvegarder vos données vers plusieurs emplacements géographiques

- faibles dépenses en capital pour la reprise après sinistre, car vous n'aurez pas à payer pour la duplication du matériel et des logiciels, ni pour les frais associés à un site de secours physique
- amélioration de la conformité des exigences réglementaires
- plus faible risque de perte de données après la restauration de vos opérations, conformément à vos accords sur les niveaux de service

4.2.4 Reprise après sinistre à titre de service

La reprise après sinistre en tant que service (DRaaS, pour *Disaster recovery as a service*) est un service offert par un fournisseur tiers ou une infrastructure infonuagique publique. Il s'agit d'une solution qui permet une réplication et un hébergement des serveurs physiques ou virtuels ainsi qu'un basculement facile entre les environnements sur place et en nuage.

Selon les accords sur les niveaux de service entre le fournisseur DRaaS et le client, les solutions suivantes peuvent être exploitées :

- surveillance, mise en œuvre et gestion de tout le PRS et aide aux clients pour le rétablissement de leurs infrastructures des TI ainsi que pour le retour aux activités normales
- temps de reprise garantis pour les ressources des TI essentielles
- outils de sauvegarde et de reprise après sinistre pour les clients qui souhaitent configurer et mettre en œuvre des solutions de reprise après sinistre sur place
- solution d'infrastructure-service, c'est-à-dire un type de service infonuagique offrant des fonctionnalités essentielles de calcul, de stockage et de réseau sur demande, sur une base de paiement à l'utilisation

4.2.5 Sauvegarde à titre de service

Une sauvegarde à titre de service est un service offert par un fournisseur tiers souvent connu sous le nom de sauvegarde en ligne ou en nuage. Le fournisseur de services peut stocker vos données à distance, dans le nuage, et gérer toute l'infrastructure de sauvegarde et de reprise pour vous.

4.2.6 Réplication du stockage

Une réplication de stockage est une copie de vos données en temps réel, d'un emplacement vers un autre, au moyen d'un réseau de stockage, d'un réseau local ou d'un réseau étendu. Puisque la réplication s'effectue en temps réel, on utilise souvent le concept de réplication synchrone pour y référer. Votre organisation peut aussi exploiter une réplication asynchrone, qui crée une copie des données au moyen d'un horaire prédéfini.

5 Résumé

Les conseils présentés dans la présente publication visent à renforcer la résilience de votre organisation grâce à une meilleure préparation en cas d'urgence. Votre stratégie de préparation en cas d'urgence doit inclure un PICI un PCA et un PRS. Les objectifs de ces trois types de plans sont très différents. Toutefois, ils partagent certains éléments en commun :

- protection de vos actifs indispensable et de vos opérations d'affaires
- intervention face aux incidents
- reprise rapide à la suite d'un sinistre

Gardez à l'esprit qu'un PICI mise sur une occurrence d'incident particulier ainsi que sur les actions requises pour y répondre, alors qu'un PRS mise sur le rétablissement de l'infrastructure des TI de votre organisation après la survenue d'une catastrophe. Les objectifs de ces deux plans visent à aider votre organisation à retourner aussi rapidement que possible à ses opérations normales.

Les principes de base d'un PICI et d'un PRS figurent sous l'égide d'un PCA. Un PCA représente une approche globale pour le traitement des interruptions. Son objectif est de maintenir les activités de votre organisation sur une base continue, pendant tout le cycle de vie de la planification.

La détermination de vos actifs indispensables et de vos activités essentielles facilitera également l'établissement de vos exigences et guidera vos processus d'élaboration de plan. Grâce à une planification efficace et à de bonnes pratiques, votre organisation sera bien préparée, prête à assurer une reprise rapide et pourra maintenir ses opérations de manière efficace. Cela vous aidera de la sorte à minimiser les impacts, les interruptions, les coûts et les dommages associés aux interruptions, aux incidents et aux sinistres qui pourraient survenir.