Direction générale adjointe

DE LA CYBERSÉCURITÉ
ET DE L'INFONUAGIQUE (DGACI)

CYBERSÉCURITÉ

Directive sur l'élaboration et l'évolution d'un plan de reprise informatique

MSSS-DIR011

2023-05-04

Votre gouvernement

Ministère de la Santé et des Services sociaux
Québec

Table des matières

Préambule

Le Réseau de la santé et des services sociaux (RSSS) ainsi que Ministère de la Santé et des Services sociaux (MSSS) offrent des services qui s'appuient fortement sur les technologies de l'information (TI). De ce fait, l'un des outils fondamentaux de la continuité de ces services est la **reprise informatique**, qui s'avère également une mesure d'atténuation des risques liés à la sécurité de l'information (SI).

Un plan de reprise informatique (PRI) est déclenché lorsque le processus de gestion des événements de sécurité ne permet pas la reprise des services dans un délai acceptable par l'organisation. Le MSSS et le RSSS doivent donc développer une capacité et une agilité de reprise informatique afin de réduire l'impact et la durée d'une éventuelle interruption qui se prolonge.

Dans ce contexte, **l'engagement formel de la haute direction** de l'organisation dans la mise en place et l'évolution de son PRI demeure un **élément majeur de réussite**.

À noter :

- ☐ La reprise informatique est un sous-ensemble d'un plan de continuité de services essentiels (PCSE). Bien que le PCSE ne fasse pas l'objet de la présente directive, la reprise informatique doit pouvoir s'y greffer.

- ☐ La reprise informatique doit s'arrimer au PCSE ainsi qu'aux processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) afin que le processus décisionnel permettant de passer du mode ***Gestion d'un événement de sécurité*** à celui de ***Plan de reprise informatique*** soit efficace et cohérent avec la GMVI.

Objectifs

Les objectifs de la présente directive se déclinent comme suit :

- préciser les rôles et les responsabilités permettant une escalade rapide, une communication concertée entre les intervenants touchés ainsi qu'une prise en charge efficace de la situation en cas d'activation du plan;
- minimiser la durée et l'impact d'éventuelles interruptions de service des actifs critiques ou du fonctionnement des systèmes informatiques qui les supportent;
- contribuer à l'adoption de bons réflexes induits par l'expérimentation des processus ainsi que par la formation et la sensibilisation des intervenants;
- favoriser l'amélioration continue du plan de reprise, notamment en tirant profit des leçons apprises lors des exercices.

Champs d'application

Cette directive s'applique aux entités suivantes :

- au MSSS;
- aux organismes publics visés au paragraphe 5 de l'article 2 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G 1.03)*, ci-après appelés « RSSS ».

Elle concerne et vise également :

- tous les domaines d'activités de ces organisations;
- toute information détenue par ces entités, native ou confiée, peu importe sa nature, le support numérique sur lequel elle se trouve ou sa localisation, et ce, durant tout son cycle de vie.

Cadre légal et administratif

Cette directive fait partie du cadre de gouvernance du MSSS et s'y inscrit, sans s'y limiter, en respect des exigences de :

- la directive sur la cybersécurité - MSSS-DIR03;
- la règle particulière sur la sécurité organisationnelle;
- le Cadre gouvernemental de référence sur la continuité des services essentiels;
- le Guide pratique pour la conception d'un plan de continuité des services essentiels;
- le Guide de la reprise informatique.

Définitions

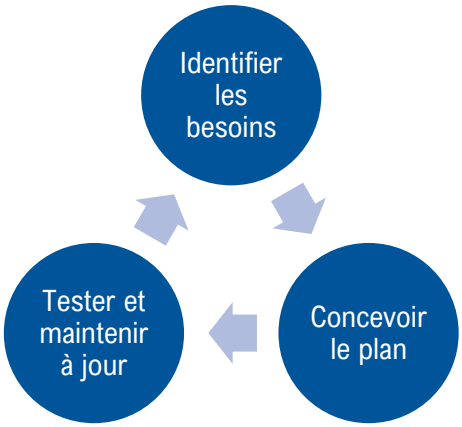
Pour l'application de la présente directive, les termes suivants signifient :

Terme	Description
Actif critique	Service dont la perturbation pourrait mettre en péril la vie, la sécurité, la santé ou le bien-être économique des personnes dans une partie ou dans l'ensemble de la population. Cette notion inclut également le service pour lequel la perturbation nuirait au bon fonctionnement des processus d'affaires de l'organisation et l'empêcherait de remplir sa mission et d'assumer ses responsabilités.
Cellule de gestion de crise	Cette cellule est le groupe décisionnel appelé à intervenir en cas de sinistre, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. Cette cellule décide de l'activation du PCSE ou du PRI.
Détenteur	Gestionnaire responsable de ressources informationnelles, conformément au Registre d'autorité de la sécurité de l'information.
Plan de continuité des services essentiels (PCSE)	Planification stratégique, tactique et opérationnelle comportant un ensemble de plans, de processus et de procédures documentés qui sont prêts à l'utilisation pour assurer l'ensemble de la continuité des services essentiels d'une organisation.

Terme	Description
Plan de reprise informatique (PRI)	Plan documenté des actions à effectuer pour relancer un service ou un ensemble de services informatiques en soutien à un processus d'affaires. C'est une composante d'un plan de continuité des services essentiels (PCSE) qui détaille des activités nécessaires au rétablissement d'un processus de gestion des technologies de l'information.
Sinistre	Événement résultant d'un ou de plusieurs aléas, pouvant causer de graves préjudices aux personnes ou d'importants dommages aux biens et exigeant de la collectivité touchée des mesures inhabituelles.

Processus soutenant le PRI

Le MSSS et le RSSS doivent déployer un processus spécifique afin de soutenir leur PRI. Ce processus comporte trois étapes : *Identifier les besoins*, *Concevoir le plan* et *Tester et maintenir à jour*. Il s'inscrit par ailleurs dans une démarche d'amélioration continue comme illustrée ci-dessous :



Fait à noter, la présente directive prévoit également des obligations **en cas d'activation** du PRI afin de compléter ce processus.

Obligations – processus soutenant le PRI

Le coordonnateur du PRI ainsi que l'équipe qui le soutient détiennent incontestablement un **rôle clé** dans la capacité de l'organisation à recouvrir le fonctionnement normal de ses actifs critiques à la suite d'une interruption prolongée de service.

Coordonnateur du PRI

Le coordonnateur élabore le PRI, le met en œuvre, en vérifie l'efficacité et le tient à jour. Ses responsabilités se déclinent ainsi :

1. Identifier les besoins

Le coordonnateur du PRI doit réaliser une analyse d'impact et la maintenir à jour, en étroite collaboration avec les détenteurs. Cette analyse consiste notamment à :

- identifier les actifs informationnels critiques ainsi que le RTO (temps d'inactivité acceptable)[1] et le RPO (perte de données acceptable)[2] pour chacun;
- établir les activités et les ressources qui soutiennent ces actifs afin de déterminer les **priorités** du PRI ainsi que la **séquence** de reprise des activités;
- faire approuver les résultats de cette analyse par le Comité de reprise informatique.

2. Concevoir le plan

Le coordonnateur du PRI conçoit le PRI dans le respect des quatre volets suivants :

➜ Développer les stratégies adéquates de reprise qui s'appuient sur les objectifs de continuité de son organisation. Ces stratégies doivent notamment déterminer :

- les ressources nécessaires (humaines, matérielles, financières, fournisseurs externes, etc.) à la bonne réalisation du PRI;
- les scénarios de sinistres auxquels les actifs critiques pourraient être exposés.

➜ Organiser la réponse à une interruption prolongée

Le coordonnateur doit mettre en place une structure de gestion adéquate pour se préparer et réagir à un événement perturbant en mobilisant du personnel qui possède l'autorité, l'expérience et les compétences nécessaires.

Cette structure doit préciser des rôles et des responsabilités attribués à des intervenants clairement désignés, et ce, pour tous les niveaux décisionnels.

Enfin, le coordonnateur doit déterminer et diffuser aux intervenants du PRI la chronologie des principales étapes d'intervention en cas de sinistre.

➜ Élaborer le PRI

Le coordonnateur doit mettre en œuvre les stratégies de reprise adoptées et s'assurer que le PRI comporte les caractéristiques suivantes :

- il est défini, connu et mis à jour en continu;
- il couvre les systèmes et réseaux d'infrastructure essentiels, en conformité avec les activités identifiées à l'analyse d'impact;
- ses critères d'activation définis et principalement basés sur l'évaluation des impacts engendrés par l'interruption de service;
- il s'appuie sur une liste à jour des coordonnées des intervenants favorisant une escalade rapide en cas d'urgence.

[1] RTO : Recovery Time Objective ou Durée maximale d'interruption admissible (DMIA)
[2] RPO : Recovery Point Objective ou Perte de données maximales admissibles (PDMA)

➜ Mettre en œuvre

Le coordonnateur s'assure que la mise en œuvre du PRI tient compte des caractéristiques suivantes :

- l'application des stratégies de reprise adoptées;
- le test de son efficacité par une mise à l'essai;
- un plan de communication spécifiant les actions à entreprendre en cas d'activation;
- sa diffusion ainsi que des actions périodiques de formation et de sensibilisation auprès de la direction, du personnel et des divers intervenants afin que ces personnes comprennent comment le plan doit être exécuté.

3. Tester et maintenir à jour

➜ Vérifier

Le coordonnateur doit réaliser des exercices périodiques[3] permettant de vérifier l'efficacité du PRI. Ces exercices doivent :

- éviter de compromettre la production;
- comporter une portée et des objectifs clairs qui serviront à évaluer la qualité de ces exercices;
- inclure un test de restauration des données et des systèmes;
- permettre de valider les numéros de téléphone des intervenants et de s'assurer que ces derniers pourront rapidement être mobilisés en cas d'activation du PRI.

➜ Maintenir à jour

Le coordonnateur doit :

- ajuster le PRI en fonction des modifications apportées aux actifs informationnels ou aux activités de l'organisation;
- mettre en place des mécanismes qui permettent d'assurer périodiquement l'exactitude des informations comprises dans le PRI, notamment la validation mensuelle des listes d'urgences liées au PRI.

➜ Produire un bilan

Le coordonnateur doit produire un bilan et un plan d'implantation des mesures correctives à la suite de chaque exercice.

Le plan des mesures correctives doit :

- mettre en évidence les éventuelles lacunes et incohérences détectées;
- être transmis au COMSI pour prise en charge des mesures correctives touchant la SI;

[3] Les exercices peuvent prendre plusieurs formes, de la simple révision documentaire à la simulation partielle ou complète d'un sinistre. Leur portée peut couvrir le PRI dans son ensemble ou se limiter à certaines de ses composantes.

- comprendre un suivi régulier et rigoureux de l'avancement de sa mise en œuvre;
- être présenté annuellement au Comité de reprise informatique.

Chef de la sécurité de l'information organisationnelle principal (CSIO principal)

Le CSIO principal a comme responsabilité :

- d'élaborer et de diffuser la présente directive au MSSS et au RSSS;
- de s'assurer qu'un coordonnateur du PRI est nommé pour le MSSS et pour chaque établissement ou organisme;
- de s'assurer du respect de la présente directive par ces organisations.

Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO est responsable de la mise en place et de l'évolution du PRI dans son organisation. À ce titre, il doit :

- prendre en charge les obligations de la présente directive;
- nommer un coordonnateur du PRI et lui apporter le soutien nécessaire afin qu'il puisse efficacement prendre en charge les responsabilités qui lui sont confiées par la présente directive, l'analyse d'impact par exemple;
- s'assurer du maintien des exigences de SI dans la préparation des activités de mise en œuvre du PRI;
- présenter annuellement l'état du plan de mesures correctives au Comité de reprise de son organisation;
- s'impliquer activement au sein de ce comité.

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI est responsable des mesures de SI. À ce titre, il doit :

- valider ou déployer les exigences de SI lors de la préparation des activités de mise en œuvre du PRI;
- collabore à l'implantation des mesures correctives liées à la SI que le coordonnateur lui aura transmis.

Détenteur

Le détenteur s'assure de la protection adéquate des actifs informationnels qui lui sont confiés. À ce titre, il doit :

- collaborer étroitement à la réalisation de l'analyse d'impact;
- s'impliquer activement au sein du Comité de reprise.

Comité de reprise informatique

Ce comité assure la coordination des activités de réponse à un sinistre. À ce titre, il doit notamment approuver :

- les résultats de l'analyse d'impact;
- le choix des actifs critiques et des priorités de reprise correspondantes;
- le PRI.

Il doit minimalement être constitué des personnes suivantes :

- le coordonnateur du PRI;
- les détenteurs touchés par le PRI;
- tout autre intervenant jugé pertinent.

Obligations - activation du plan de reprise

Cellule de gestion de crise

Cette cellule est le groupe décisionnel qui intervient en cas de sinistre, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services.

Cette cellule décide de l'activation du PRI de l'organisation et, sur recommandation du Comité de reprise, confirme le retour à la normale des activités en mode non dégradé.

Comité de reprise informatique

Le Comité de reprise informatique détient la responsabilité :

- d'activer le PRI à la demande de la cellule de gestion de crise;
- de prendre les mesures nécessaires afin de neutraliser toute entrave au bon déroulement du PRI soumise par le coordonnateur du PRI.

Coordonnateur du PRI

Le rôle du coordonnateur demeure déterminant dans le déploiement du PRI et de ses composantes en cas d'activation. À ce titre, il doit notamment :

- veiller à ce que les services critiques redeviennent disponibles à l'intérieur des délais convenus dans l'analyse d'impact;
- coordonner le déploiement du PRI et gérer les relations avec les fournisseurs externes de ressources technologiques;
- formuler au Comité de reprise tout besoin ad hoc en matière de ressources (humaines, matérielles, financières, etc.) ainsi que toute situation nécessitant une décision;
- rédiger, dès le retour à la normale, un bilan visant à informer le Comité de reprise informatique du déroulement de l'incident.

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI est responsable de l'application des mesures de SI. À ce titre, il doit :

- s'assurer que les mesures sont maintenues à la suite de l'activation du PRI;
- transmettre au coordonnateur du PRI toute vulnérabilité qu'il constate à la suite de son activation.

Entrée en vigueur et révision

Cette directive entre en vigueur à la date de son approbation. Elle doit être révisée :

- tous les trois ans;

  ou

- lors de changements organisationnels ou de l'adoption de nouvelles orientations ministérielles en matière de plan de reprise informatique.

Approuvée par le chef délégué de la sécurité de l'information (CDSI) :	Reno Bernier
Date d'approbation :	4 mai 2023