UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide du plan de sauvegarde

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Table des matières

INTRODUCTION 3

1.1 CONTEXTE 3

1.2 OBJECTIF 3

1.3 PORTÉE 3

2 LE PLAN DE SAUVEGARDE 4

2.1 QU'EST-CE QU'UN PLAN DE SAUVEGARDE DES DONNÉES? 4

2.2 POURQUOI EST-IL IMPORTANT? 4

3 LES DIFFÉRENTES ÉTAPES À SUIVRE POUR RÉALISER UN PLAN DE SAUVEGARDE INFORMATIQUE EFFICACE 4

3.1 DÉFINIR LES INFORMATIONS À PROTÉGER EN PRIORITÉ 4

3.2 LES MÉTHODES DE SAUVEGARDE 5

3.3 FRÉQUENCE DES SAUVEGARDES 6

3.4 STRATÉGIE DE SAUVEGARDE 6

3.5 TESTER LA PROCÉDURE DE SAUVEGARDE 7

3.6 DOCUMENTER LA PROCÉDURE DE SAUVEGARDE 8

3.7 PROTECTION DES SAUVEGARDES ET DES SUPPORTS DE SAUVEGARDE 8

3.8 CONSERVATION ET ÉLIMINATION DES SAUVEGARDES ET DE LEURS SUPPORTS 9

3.9 EMPLACEMENTS DES SUPPORTS DE SAUVEGARDE ET LEURS TRANSPORTS HORS SITE 9

4 LA MATRICE RACI 9

5 DÉFINITIONS 11

6 SOURCES 11

7 RÉVISIONS 11

INTRODUCTION

1.1 CONTEXTE

Chaque établissement a la responsabilité de protéger adéquatement tous les actifs de son établissement, qu'ils soient numériques ou non. Il peut s'agir de données administratives, financières, personnelles ou autres. De nos jours, il existe des menaces telles que les incendies, les catastrophes naturelles, le vol de matériel, le piratage, les virus informatiques, le dysfonctionnement du matériel informatique, les erreurs humaines qui peuvent conduire à une fuite, une modification non autorisée ou à une suppression de données du réseau de l'Université du Québec (UQ). Pour éviter toutes ces déconvenues, il est donc conseillé de mettre en place un plan de sauvegarde informatique.

La sauvegarde des informations constitue la principale ligne de défense des établissements, en particulier nos établissements, en cas de perte ou de modification accidentelle ou malveillante des informations, des applications et des configurations d'infrastructure. Elle contribue fortement à assurer la continuité des activités des établissements. Il est donc impératif de s'assurer qu'elles soient effectuées selon les meilleures pratiques de sécurité afin de garantir que l'intégrité des données sauvegardées permette une restauration cohérente en tout temps.

Le Centre d'expertise en sécurité de l'information (CESI) a décidé de créer un guide de recommandations d'un plan de sauvegarde afin que les établissements puissent s'en inspirer et par la suite, créer leur propre plan.

1.2 OBJECTIF

Le présent document vise à préciser les exigences de sécurité entourant la sauvegarde, la rétention, la restauration des actifs des établissements du Québec et décrit de manière explicite la méthode utilisée, ainsi que les étapes nécessaires pour la réalisation d'un bon plan de sauvegarde des données d'établissements, afin de s'assurer de leur disponibilité et de leur intégrité en tout temps.

=

1.3 PORTÉE

Ce document s'adresse à tous les établissements d'enseignement supérieur, aux détenteurs de l'information, aux professionnels de la sécurité de l'information et à toutes les ressources qui seront sollicitées dans la démarche du plan de sauvegarde des actifs de l'établissement.

2 LE PLAN DE SAUVEGARDE

2.1 QU'EST-CE QU'UN PLAN DE SAUVEGARDE DES DONNÉES?

Le plan de sauvegarde de données définit la stratégie adoptée par tout établissement pour dupliquer et sécuriser toutes les données qui sont contenues dans son système informatique. Tout établissement, qu'importe sa taille, a besoin d'une procédure de sauvegarde de données.

Il décrit également le processus de restauration à respecter. C'est d'ailleurs pourquoi il va de pair avec :

- Le plan de reprise des activités (PRA), constitué du plan de reprise informatique (PRI), se définit comme un ensemble de procédures, dont l'objectif est de prévoir comment redémarrer le plus rapidement possible l'activité professionnelle en cas d'incident informatique (catastrophes naturelles, accidents humains, panne matérielle ou logicielle, vol, cybercriminalité, etc.).

- Le plan de continuité des activités (PCA) qui est un ensemble de procédures documentées servant de guide aux établissements pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation.

2.2 POURQUOI EST-IL IMPORTANT?

Il nous permet de disposer d'une ou plusieurs copies de sauvegarde pour la restauration des données en cas d'incident entraînant une perte de celles-ci (attaque informatique, sinistre, catastrophe naturelle, erreur humaine, etc.).

Il est donc indispensable pour les établissements qui souhaitent exercer en totale sécurité de disposer d'une solide stratégie. Celle-ci permettra de :

- Réduire au maximum le temps d'arrêt;
- Limiter les pertes financières découlant de la disparition des informations;
- Protéger autant que possible de l'impact négatif d'un tel évènement sur l'image de votre établissement.

3 LES DIFFÉRENTES ÉTAPES À SUIVRE POUR RÉALISER UN PLAN DE SAUVEGARDE INFORMATIQUE EFFICACE

3.1 DÉFINIR LES INFORMATIONS À PROTÉGER EN PRIORITÉ

La première étape pour mettre en place un plan de sauvegarde informatique consiste à identifier et à sélectionner les informations qui devront être protégées. Il faudra recenser les données, et cartographier les différents éléments à sauvegarder de manière à établir un ordre de priorité des données, des plus importantes, aux moins importantes. Cette première étape permet de classer toute l'information qui devra être sauvegardée.

Dans la mesure du possible, mieux vaut conserver l'ensemble de vos informations, car toutes sont susceptibles de revêtir de forts enjeux puisque, .on ne sait jamais à l'avance lesquelles deviendront la cible privilégiée des pirates informatiques. Cependant, en fonction de vos possibilités et des ressources dont vous disposez, vous pouvez choisir de favoriser les informations à sauvegarder en identifiant celles dont la perte impacterait le plus négativement votre établissement. Ces données clés sont également celles à restaurer en premier en cas de problème.

Il est de la responsabilité du détenteur des données d'identifier les données qui sont critiques et qui doivent être sauvegardées. Cette identification est capturée en tant qu'exigences pendant le cycle de mise en œuvre d'un système ou d'un service. Une évaluation formelle des risques et une analyse d'impact sur l'activité doivent être entreprises pour déterminer les exigences pour tous les plans de sauvegarde et de récupération des données. Les analyses de risques et analyse d'impact sur l'activité doivent être mises à jour au moins une fois par an pour s'assurer qu'elles sont conformes aux exigences de l'établissement et de ses technologies.

3.2 LES MÉTHODES DE SAUVEGARDE

Le plan des 18 mesures minimales du MCN rend obligatoire la prise de copies quotidienne. Les sauvegardes doivent être automatisées. Il existe différentes méthodes :

- **Complète**

Chaque fichier du système est copié et assemblé en un seul fichier. Ce fichier qui contient des copies de sauvegarde de l'ensemble du système peut être très volumineux et occuper beaucoup d'espace.

- **Incrémentale**

Tous les fichiers qui ont été modifiés après la dernière sauvegarde que vous avez effectuée sont sauvegardés.

- **Différentielle**

Les fichiers qui ont été modifiés ou altérés depuis une sauvegarde complète sont sauvegardés.

- **Différence entre différentielle et incrémentale**

La différence la plus importante entre les sauvegardes incrémentales et différentielles est le temps nécessaire pour restaurer les données en cas d'urgence :

- Si vous utilisez une combinaison de sauvegardes complètes et différentielles, vous ne devrez restaurer que deux sauvegardes : la sauvegarde complète la plus récente et la sauvegarde différentielle la plus récente.
- Si vous utilisez une combinaison de sauvegardes complètes et de sauvegardes incrémentales, vous devrez restaurer la sauvegarde complète la plus récente ainsi que toutes les sauvegardes incrémentales effectuées depuis cette sauvegarde complète.

EXEMPLE

- Situation 1

Dans la première situation, une sauvegarde complète est exécutée le lundi soir, puis des sauvegardes différentielles sont effectuées tous les autres soirs de la semaine. **Si une panne survient le samedi matin, il faudra restaurer la sauvegarde complète du lundi, puis seulement la sauvegarde différentielle du vendredi.**

- Situation 2

Dans la deuxième situation, une sauvegarde complète est exécutée le lundi soir et des sauvegardes incrémentales sont effectuées toutes les autres nuits de la semaine. **Si une panne survient le samedi matin, il faudra restaurer la sauvegarde complète du lundi, puis chaque sauvegarde incrémentielle dans l'ordre chronologique d'origine.**

3.3 FRÉQUENCE DES SAUVEGARDES

Elles doivent être effectuées sur une base planifiée pour répondre aux paramètres d'objectifs de temps de récupération (RTO) et d'objectifs de point de récupération (RPO).

Si aucun RTO ou RPO spécifique n'est défini, le RTO (24 heures) et le RPO (48 heures et plus) par défaut doivent s'appliquer.

Une sauvegarde complète doit être effectuée avant chaque modification majeure d'un composant matériel ou logiciel (système ou application) et avant chaque changement majeur de configuration. Elle doit aussi être effectuée après chaque modification majeure si elle n'est pas déjà prévue dans le plan de sauvegarde.

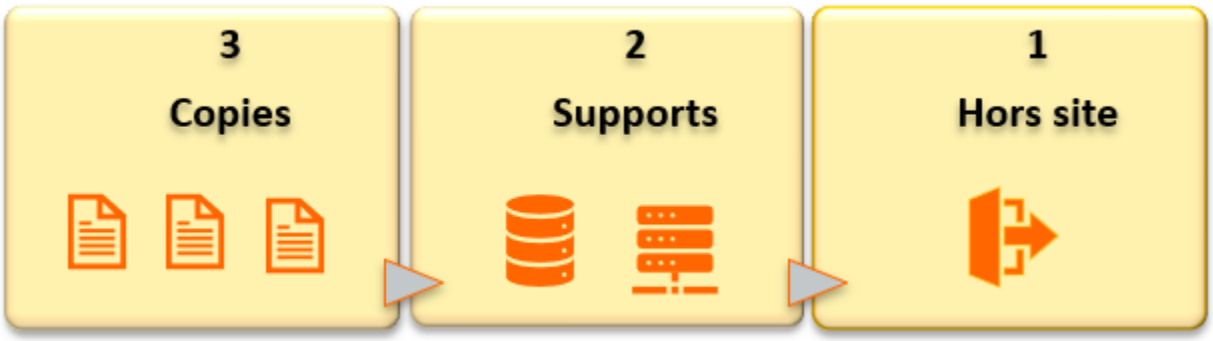
3.4 STRATÉGIE DE SAUVEGARDE

Pour une stratégie complète, il faut réaliser des sauvegardes journalières, hebdomadaires et mensuelles.

a) La stratégie du 3-2-1

Elle consiste à :

- Réaliser **3** copies de données (1 original et 2 copies);
- Stockées sur deux (**2)** supports différents;
- Avec une (**1**) copie située sur un site distant.



b) La stratégie du 3-2-1-1-0

Elle consiste à :

- Réaliser **3** copies de données (1 original et 2 copies);
- Stockées sur deux (**2)** supports différents;
- Avec une (**1**) copie située sur un site distant;
- Au moins une (**1**) copie est hors ligne et disponible pour toute récupération;
- Et contient (**0**) erreur.

3.5 TESTER LA PROCÉDURE DE SAUVEGARDE

L'une des étapes importantes de tout processus de sauvegarde est d'effectuer des tests.

En avoir une, .ne signifie pas nécessairement qu'elle est viable et peut être restaurée lorsque le besoin se fera sentir. Elles doivent être testées régulièrement pour s'assurer qu'on puisse restaurer les données au besoin. Un échantillon de travaux de sauvegarde doit être vérifié dans le cadre du processus visant à maintenir l'intégrité des informations traitées.
4
Les rapports d'échec doivent être produits, examinés et traités dans un délai raisonnable pour garantir le succès de l'opération. Ces rapports doivent être envoyés au système de corrélation des évènements de l'établissement. Le CESI préconise que des tests soient réalisés de manière régulière pour vérifier l'intégrité des sauvegardes.

3.6 DOCUMENTER LA PROCÉDURE DE SAUVEGARDE

La procédure doit être formellement documentée, approuvée et communiquée aux personnes appropriées. Elle doit aussi être révisée régulièrement à des fréquences définies par chaque établissement.

Des copies sur support papier et/ou électronique de la procédure doivent être conservées à l'extérieur de l'établissement et disponibles en cas de désastre ou d'incapacité d'y accéder depuis les locaux de l'établissement.

Le personnel de l'exploitation doit aussi être formé sur les processus de sauvegarde et de restauration.

Pour s'assurer d'être prêt à réagir en cas d'incident majeur, du personnel additionnel de l'exploitation doit être formé sur le processus de restauration ou du personnel d'exploitation connaissant le processus de restauration doit être identifié dans d'autres sites d'exploitation de l'établissement.

3.7 PROTECTION DES SAUVEGARDES ET DES SUPPORTS DE SAUVEGARDE

Les supports de sauvegarde doivent être traités comme étant d'un niveau de classification équivalent à celui du système d'information source ou de la donnée sauvegardée.

Les copies des données sauvegardées doivent être chiffrées par un algorithme et une méthode de chiffrement autorisés par l'établissement afin d'être protégés contre des personnes malveillantes.

Les secrets pour le chiffrement doivent être gérés de manière sécuritaire (par le biais d'une voûte).

L'accès aux supports de doit être limité au personnel autorisé uniquement comme le prévoit la clause sur les rôles et responsabilités.

Toute copie d'une donnée classifiée confidentielle doit conserver cette propriété durant tout son cycle de vie.

Le système doit être migré dans un environnement réseau séparé et accessible uniquement aux personnes dument autorisées.

Les équipements de sauvegarde doivent pouvoir transmettre des données au nuage, aucune communication entrante ne doit être autorisée.

Ne pas autoriser l'accès Internet entrant aux sauvegardes des données et les séparer des autres équipements du réseau informatique afin qu'une infection de celles-ci ne compromettre pas leur intégrité, disponibilité et la confidentialité.

3.8 CONSERVATION ET ÉLIMINATION DES SAUVEGARDES ET DE LEURS SUPPORTS

Les supports de sauvegarde doivent être conservés conformément aux exigences de récupération informatique, de conservation des données et de gestion des enregistrements, le cas échéant.

Ils doivent être éliminés conformément aux exigences d'élimination appropriées décrites en fonction des bonnes pratiques et de la sensibilité des données, par exemple en écrasant les supports ou en le détruisant physiquement selon un processus vérifié et auditable.

Pour plus d'information sur la conservation et l'élimination des sauvegardes, veuillez consulter le calendrier de conservation et de destruction: Recueil-des-règles-de-conservation_docs_univ_QC_BCI.pdf (bci-qc.ca)

3.9 EMPLACEMENTS DES SUPPORTS DE SAUVEGARDE ET LEURS TRANSPORTS HORS SITE

Les supports contenant des informations sensibles ne doivent être transportés hors site qu'avec une protection physique appropriée, dans un conteneur sécurisé, à l'intérieur d'un véhicule sécurisé, suivant un processus vérifiable.

La fréquence d'envoi de ces supports hors site doit être documentée et justifiée dans le calendrier de sauvegarde. Le choix de la fréquence doit tenir compte de l'importance et des exigences de récupération des données.

Ils doivent aussi être stockés dans un emplacement physique sécurisé pour garantir que les supports sont protégés contre l'accès, la modification ou la destruction non autorisés. Ceci comprend:

- Dans un site en dehors de celui de l'établissement et stocké dans un endroit avec une sécurité physique stricte en place.
- Dans un environnement à température contrôlée utilisant des mécanismes de suppression des incendies.
- Dans des coffres-forts désignés de l'établissement, pour le stockage local des supports de sauvegarde.

4 LA MATRICE RACI

Vous trouverez ci-dessous un exemple de tableau RACI que vous pourriez utiliser, modifier et adapter à vos propres besoins.

- R : responsable (en charge de);
- A : approbation;
- C : consulté/contributeur;
- I : informé.

	CSIO	Détenteur	Analyste Cybersécurité	Responsable Infra. Techno	Équipes d' exploitation	Responsable de la continuité
Classifier l'information à sauvegarder	I	A	R			
Définir le RTO et le RPO des données à sauvegarder	I	A	C		R	
Définir le RTO et le RPO par défaut	A	C	C	I	C	R
Effectuer le plan de sauvegarde de l'actif	I	A	C	I	R	
Mettre en œuvre le plan de sauvegarde de l'actif	I	I	I	A	R	
Prendre en charge les erreurs de sauvegarde	I	I	C	A	R	
Effectuer la reprise en cas sinistre	I	A	C	I	R	R
Surveiller les journaux de sauvegarde	I		R	A	C	
Réaliser le processus de sauvegarde et de restauration des données de l'établissement suivant la planification établie	I	I	C	A	R	I
Réaliser la procédure de sauvegarde de chaque actif	I	I	C	A	R	
Former le personnel additionnel sur le processus de sauvegarde et de restauration annuellement	I	I	C	A	R	I
Effectuer les vérifications de la réussite de sauvegardes sur chaque actif sauvegardé	I	I	C	A	R	I
Établir le calendrier de sauvegarde et de test de restauration	A	I	C	I	R	R
Effectuer les tests de recouvrement des sauvegardes selon le calendrier et produire un rapport de restauration au détenteur/propriétaire	I	A	I	I	R	R
Entreposer les médias dans un endroit sécuritaire	I		I	A	R	C
Planifier les tests de simulation de reprise après sinistre	I	I	C	A	R	
Réaliser les simulations de reprise	A	I	C	I	R	
Produire un rapport de la simulation avec des recommandations	A	I	C	I	R	
Définir la fréquence d'envoie des copies de sauvegarde	A		C	I	R	

5 DÉFINITIONS

Copie de sauvegarde : Information enregistrée sur un support de stockage.
Objectif de point de reprise (RPO) : fait référence à la quantité maximale de données qui pourraient être perdues sans compromettre la continuité de fonctionnement de votre établissement. Par exemple, si le RPO de votre établissement est de cinq heures, votre système doit sauvegarder les données au moins toutes les cinq heures.
Objectif de temps de récupération (RTO) : fait référence au temps maximum après un sinistre qu'un système ou un service soit restauré. Il s'agit du temps que l'établissement peut tolérer sans accès aux données ou aux systèmes critiques. Si le RTO de votre établissement est de deux heures, elle ne peut pas se permettre de rester à l'arrêt plus longtemps.
Temps d'arrêt maximal tolérable (**MTD**) : c'est la durée pendant laquelle l'entreprise peut être arrêtée sans que cela n'affecte ses /activités. RTO < ou = MTD.
Bilan d'impact sur les activités (BIA) : identifie les ressources essentielles à votre établissement et évalue la probabilité et l'impact de chaque menace.
Un évènement de sécurité : tout évènement, acte, omission ou situation susceptible de nuire à =la sécurité de votre établissement.
Incident de sécurité : Un événement qui compromet réellement ou de manière imminente, la confidentialité, l'intégrité ou la disponibilité d'informations ou d'un système d'information.

6 SOURCES

https://www.apog.net/plan-de-sauvegarde-informatique#:~:text=Le%20plan%20de%20sauvegarde%20informatique%2C%20%C3%A9galement%20connue%20sous%20le%20nom,donn%C3%A9es%20informatiques%20d'une%20soci%C3%A9t%C3%A9.
https://www.veritas.com/fr/ca/information-center/data-backup-and-recovery
https://blogs.manageengine.com/fr/2023/04/11/guide-de-sauvegarde-pour-un-reseau-resistant-aux-risques.html
https://www.apog.net/plan-de-sauvegarde-informatique
https://www.groupesl.com/nouvelles/comment-creer-plan-sauvegarde-donnees/
https://microage.ca/fr/les-meilleures-pratiques-de-sauvegardes-des-donnees/
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/economie/contenu/continuite_activites/GM_guide_gestion_continuite_activites.pdf

7 RÉVISIONS

Date	Action	Auteur	Ver.
2023-10-15	Version courante	CESI de l'UQ	0.9
2024-01-22	Ajustement du TLP	Jean-François Blais	1.1