UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Aide-mémoire
Plan de reprise informatique

Mars 2024

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIÈRES

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

OBJECTIF DU PLAN DE REPRISE INFORMATIQUE

L'objectif du plan est de déterminer la résilience requise de l'infrastructure et de conduire l'élaboration de plans de reprise après sinistre et d'urgence informatique. Le plan aborde la structure organisationnelle de la gestion de la reprise, couvrant les rôles, les tâches et les responsabilités des prestataires de services internes et externes et les processus de planification qui créent les règles et les structures pour documenter, tester et exécuter la reprise après sinistre. Le plan couvre aussi des éléments tels que l'identification des ressources critiques, la notation des dépendances clés, la surveillance et les principes de sauvegarde et de récupération.

PLAN DE REPRISE INFORMATIQUE

Le plan de reprise informatique est conçu pour réduire l'impact d'une interruption majeure sur les activités clés de l'établissement. Ces activités sont basées sur la compréhension des risques liés aux impacts potentiels sur l'entreprise. Le plan de reprise répond aux exigences de résilience, de traitement alternatif et de capacités de récupération de tous les services informatiques critiques. Il doit également couvrir les directives d'utilisation, les rôles et les responsabilités, les procédures, les processus de communication et l'approche de test.

RESSOURCES INFORMATIQUES CRITIQUES

L'attention doit principalement être portée sur les éléments spécifiés dans le plan de continuité des services essentiels mentionnés dans le formulaire des plans de reprise des affaires afin de renforcer la résilience et établir des priorités dans les situations de reprise.

Lors d'une situation de reprise, les distractions doivent être évitées et il faut s'assurer d'une réponse et d'une récupération conforme aux besoins prioritaires de l'établissement, tout en veillant à ce que les coûts soient maintenus à un niveau acceptable et conforme aux exigences réglementaires et contractuelles. Les exigences de résilience, de réponse et de récupération pour différents niveaux doivent être respectées sur une ligne de temps établie. Par exemple :

- Une à quatre heures
- Quatre à 24 heures
- Plus de 24 heures
- Les périodes opérationnelles critiques

Aussi, les établissements doivent prendre en considération les éléments importants ci-dessous :

- **Point de récupération des données (RPO)** : Point à partir duquel les données utilisées par une activité doivent être restaurées afin de permettre la reprise du fonctionnement (retour à la normale).
- **Objectif du délai de rétablissement (RTO)** : Durée nécessaire après un incident pendant laquelle un service ou une activité sont repris, ou des ressources sont rétablies.

INFRASTRUCTURES

- L'existence d'un schéma de réseau à jour et de l'inventaire des actifs informatiques :
  - Lignes voix et données
  - Configuration
  - Utilisation principale (données ou voix)
  - Identification et information du fournisseur
  - Équipements réseau (sur site et hors site)
  - Dispositions de basculement
  - Applications critiques prises en charge
- La stratégie des installations (site chaud, site froid, etc.) et déterminer s'il y a des dispositions dans la stratégie pour l'équipement de communication.
- La préparation d'une liste des applications critiques, des ressources relatives (serveur, système d'exploitation, réseaux, stockage, etc.) et de l'ordre de priorité pour leur restauration.

- La redondance pour l'alimentation électrique des sites principaux et distants et aussi l'autonomie des générateurs de secours et des onduleurs doivent être assurées.
- Les étapes des mesures de reprise des communications contenues dans le plan de reprise informatique doivent être examinées.
- L'existence d'un contrat pour un emplacement hors site et la détermination, s'il inclut des engagements pour la maintenance réseau, doivent être validées.
- Les contrats avec les fournisseurs de communication doivent être examinés et leur engagement à restaurer les capacités de l'infrastructure doit être déterminé.
- Lorsqu'un système téléphonique sur le site est installé, il faut confirmer l'existence d'autres lignes téléphoniques extérieures pour la redondance.

RÉCUPÉRATION DE DONNÉES

- Conserver adéquatement les sauvegardes de données clés et de systèmes d'exploitation hors site.
- Tester régulièrement les procédures de restauration des données et des systèmes d'exploitation.
- Inclure les postes de travail qui constituent l'interface utilisateur des applications dans le processus de sauvegarde.
- Confirmer la capacité de la plate-forme de restauration à rétablir physiquement les données dans le délai prescrit.
- Vérifier la disponibilité de la sauvegarde des données, de même que le transport de celles-ci vers le site de traitement provisoire dans le délai établi dans le plan de reprise informatique.
- S'assurer de l'élaboration et de la documentation des procédures pour gérer la récupération des données perdues entre la dernière sauvegarde et le moment du sinistre.

REPRISE DES INSTALLATIONS

- Analyser le besoin de l'espace nécessaire aux opérations (si applicable).
- Prendre en compte l'espace de récupération pour toutes les solutions internes et externes, lors de l'élaboration de ce plan.
- Vérifier que le plan répond aux besoins d'alimentation électrique redondante pour la reprise (sources d'alimentation sans coupure, générateurs de secours).

GESTION DU PERSONNEL

- Documenter clairement la structure organisationnelle des équipes de reprise.
- Communiquer et sensibiliser les responsabilités aux membres de l'équipe (intervention et reprise).
- Inclure une procédure pour contacter le personnel et rendre compte de tous les membres du personnel après une catastrophe.
- Avoir des procédures pour le recrutement de personnel temporaire, d'autres emplacements ou organisations, si les membres du personnel principal ne sont pas disponibles.
- Mettre en place des dispositions permettant au personnel hors site d'accéder aux mots de passe critiques, de traiter avec les fournisseurs et de libérer des supports de sauvegarde en cas d'indisponibilité du personnel sur le site.
- Prévoir l'hébergement temporaire et le transport dans le plan de relocalisation du personnel.
- Posséder les informations de contact telles que les numéros de téléphone et le lieu de travail des ressources clés.

PROCÉDURES

Les procédures de récupération doivent être suffisamment détaillées pour que le personnel n'appartenant pas à l'entreprise puisse effectuer les tâches de récupération. Les procédures doivent inclure des détails sur les éléments suivants :

- La présentation de l'environnement informatique (interfaces et fonctionnalités).
- La présentation de la récupération.
- Les conditions préalables à la récupération (exigences matérielles minimales, systèmes, manuels, configurations de pare-feu, mots de passe).
- L'évaluation des dommages.
- Les étapes de récupération (physique, réseau, système d'exploitation, application, base de données).
- Le processus de vérification post-récupération.
- Les procédures de maintien du service en mode récupération.
- Les procédures de transition vers un site de récupération principal.
- Les procédures de restauration sur un site permanent.
- Les moyens pour informer, le personnel concerné, des pannes de télécommunication, d'électricité et de plate-forme.

- Les dispositions pour le déploiement immédiat du personnel technique en cas d'indisponibilité du personnel principal.

L'existence des étapes d'évaluation des dommages avec des points de décision formels et des seuils pour activer le plan est validée ainsi que la confirmation de la réponse est proportionnée à l'impact de l'incident.

FOURNISSEURS TIERS (SI APPLICABLE)

Contrôle : les fournisseurs tiers qui exécutent des processus métier sont inclus dans le plan de reprise informatique ou dans un autre plan distinct spécifique au fournisseur. Les deux approches souscrivent aux mêmes politiques, normes, directives et procédures que les processus exécutés en interne.

- S'assurer que les contrats des fournisseurs incluent des exigences du plan de reprise informatique.
- S'assurer que les sous-traitants du fournisseur sont inclus au plan de reprise informatique de l'entreprise ou dans un document ou un accord spécifique au fournisseur.
- S'assurer que le plan de reprise informatique des fournisseurs souscrit aux mêmes politiques, normes et directives internes à votre établissement pour l'évaluation des risques, la récupération matérielle et logicielle, la récupération des données et la récupération des installations.
- S'assurer que les contrats avec des tiers incluent des accords de niveau de service (SLA) pour l'intérim et la restauration des services.
- S'assurer que le plan de reprise informatique spécifique au fournisseur est régulièrement testé.

À la lumière de ces résultats : évaluer l'efficacité du plan de reprise informatique du fournisseur.

MAINTIEN DU PLAN DE REPRISE INFORMATIQUE

- Définir et exécuter les procédures de contrôle des changements pour s'assurer que le plan de reprise informatique est tenu à jour et reflète en permanence les exigences opérationnelles prévues.
- Communiquer clairement et en temps opportun les changements de procédures et de responsabilités.
- Déterminer les responsables du maintien du plan et de l'examen des procédures de maintenance et de révision.

ESSAIS DU PLAN DE REPRISE INFORMATIQUE

Ce plan doit être mis à l'essai régulièrement pour s'assurer que les systèmes informatiques peuvent être récupérés efficacement, que les lacunes sont corrigées et que le plan reste pertinent. Cela nécessite une préparation minutieuse, une documentation, un compte-rendu des résultats des essais et, en fonction des résultats, la mise en œuvre d'un plan d'action. Il faut aussi tenir en compte la portée des essais de récupération des actifs, la prise en considération des scénarios multiples et l'intégration de fournisseurs externes aux essais.

FORMATION AU PLAN DE REPRISE INFORMATIQUE

Toutes les parties concernées doivent être formées sur les procédures, leurs rôles et responsabilités, en cas d'incident ou de catastrophe. Cette formation doit être vérifiée et améliorée en fonction des résultats des tests de contingence.

DISTRIBUTION DU PLAN DE REPRISE INFORMATIQUE

Une stratégie de distribution doit être définie et gérée pour s'assurer que les plans soient distribués à toutes les parties prenantes. Les plans devront être accessibles, quel que soit le scénario de catastrophe.

RÉCUPÉRATION ET REPRISE DES SERVICES INFORMATIQUES

Une planification des actions à entreprendre est primordiale à la récupération et à la reprise des services informatiques. Cela peut inclure l'activation de sites de secours, le lancement d'un traitement alternatif, la communication avec les clients et les parties prenantes ainsi que les procédures de reprise.

ENTREPOSAGE HORS SITE

Une copie de tous les supports de sauvegarde critiques, de la documentation et des autres ressources informatiques nécessaires au plan de reprise informatique doit être conservée hors site.

L'équipe de reprise doit veiller à ce que les dispositions hors site soient évaluées périodiquement, au moins une fois par an, en matière de contenu, de protection de l'environnement et de sécurité.

Important : S'assurer de la compatibilité du matériel et des logiciels pour restaurer les données sauvegardées ou archivées.

EXAMEN POST-INCIDENT

L'équipe de reprise doit évaluer l'adéquation du plan de la reprise informatique. Le bilan post-incident permet l'ajustement du plan de reprise par le biais de recommandations.

PLAN DE COMMUNICATION

S'assurer qu'un plan de communication est en place et que le rôle et les responsabilités de la Direction des communications sont définis.

- L'importance de la priorisation des processus de communication ainsi que la définition de la responsabilité de la communication. Par exemple :
  - Public
  - Presse
  - Gouvernement

Pour plus de détails aux informations nécessaires, veuillez prendre connaissance de « l'Annexe A » à la fin de ce document.

CYBER-ASSURANCE

Une cyberassurance est recommandée afin de mieux gérer les situations en cas d'atteinte, d'attaque informatique ou de fuite de données.

Selon le contrat souscrit, cette assurance prend en charge une partie ou l'ensemble des pertes d'exploitation occasionnées en cas d'interruption ou de diminution de l'activité de votre établissement à la suite d'une défaillance ou de l'altération de votre système informatique.

Durant la souscription, il faut répondre à un seuil d'exigence et de point de conformité afin d'être assurable. Dans le cas où l'établissement serait assurable, le montant de la prime est corrélé avec le niveau de la maturité des procédures, de leur conformité aux bonnes pratiques en matière de la gestion et de la maintenance des systèmes d'information.

ANNEXE A

Voici la liste des coordonnés à maintenir :

- Les parties prenantes concernées, par exemple :
  - L'équipe de gestion de crise
  - Le personnel de récupération informatique
  - Les parties prenantes de l'établissement
  - Le personnel

- Les fournisseurs de services, par exemple :
  - La liste des fournisseurs
  - L'opérateur de télécommunication

- Les parties externes, par exemple :
  - Les partenaires commerciaux
  - Les médias
  - Les organismes gouvernementaux
  - Le public

N. B. : Les informations pertinentes sont identifiées, saisies et communiquées au moment opportun pour les différentes parties prenantes et dans un délai qui permet aux personnes de s'acquitter de leurs responsabilités. Une communication efficace se produit également dans un sens plus large, circulant vers le bas, transverse et vers le haut de l'établissement.

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

RÉVISIONS

Date de révision : 2024-03-13