Plan de Secours pour le Laboratoire GSB

1. Objectifs du Plan de Secours

Le plan de secours vise à assurer la continuité des activités critiques du laboratoire GSB en cas d'incident majeur affectant l'infrastructure informatique ou les opérations de l'entreprise.

2. Identification des Sinistre

Sinistre	Risques	Impact	Priorité	Type
Panne électrique prolongée	Modéré	Élevé	4	Technique
Cyberattaque	Modéré	Très Élevé	1	Technique
Panne matérielle des serveurs	Modéré	Élevé	2	Technique
Incendie	Modéré	Élevé	3	Sécuritaire
Inondation	Faible	Moyen	8	Sécuritaire
tremblement de terre.	Faible	Très Élevé	5	Sécuritaire
Pandémie ou crise sanitaire	Faible	Élevé	6	Opérationnelles
Problème logistique affectant les visiteurs médicaux	Faible	Modéré	8	Opérationnelles
Perte de retour sur investissement dans des machines médicales, Non ou peu utiliser au finale	Faible	Faible	9	Financière
Mise en place d'une nouvelle technologie qui ne convient finalement pas	Faible	Élevé	7	Stratégique

3. Priorisation des Activités Critiques

Accès aux bases de données pharmaceutiques (BDMED, BDPHARMA)

Fonctionnement du réseau et des systèmes de communication

Accès à la messagerie professionnelle et aux outils collaboratifs

Gestion des ressources humaines et des frais de déplacement des visiteurs

Systèmes de sécurité (contrôle d'accès, surveillance)

4. Plan de sauvegarde

4.1. Types de sauvegarde: avantages et inconvénients

Full backup (Sauvegarde complète)	Un fichier qui contient une image complète d'un disque entier. Avantages: c'est le seul fichier nécessaire pour récupérer un disque entier. Inconvénients: Grande taille.
Differential (Différentiel)	Un fichier qui contient la différence entre les données actuelles du disque et la dernière sauvegarde complète. Avantages: plus petite qu'une sauvegarde de disque complète. Inconvénients: généralement plus volumineux qu'une sauvegarde incrémentielle. Nécessite une sauvegarde différentielle et une image de sauvegarde complète pour restaurer un disque.
Incremental (Incrémentation)	Un fichier qui contient la différence entre les données actuelles du disque et la dernière sauvegarde (complète, différentielle ou incrémentielle). Avantages: plus petite taille, par rapport à une sauvegarde différentielle ou complète.

	Inconvénients: peut nécessiter plusieurs images de sauvegarde incrémentielle / différentielle en plus d'une sauvegarde complète pour restaurer les données. Si l'un des fichiers de sauvegarde incrémentielle est corrompu, les données stockées dans les fichiers de sauvegarde incrémentielle ultérieurs ne peuvent pas non plus être restaurées.

Redondance des données : réplication quotidienne des informations aux États-Unis

Serveurs de secours : mise en place de serveurs répliqués en dehors du site principal

Sauvegardes régulières : sauvegardes incrémentales toutes les 6 heures

Virtualisation : migration vers un environnement hautement virtualisé pour une reprise rapide

Dupliqué les données : Copier les données dans un datacenter sécuriser externe

5. Mesures de Prévention et de Protection

5.1. Cybersécurité

Pare-feu et systèmes de détection d'intrusion (IDS/IPS)

Formation et sensibilisation des employés aux cybermenaces

Plan de réponse aux cyberattaques avec une équipe d'intervention dédiée

Double authentification (2FA) pour les accès aux systèmes critiques

5.2. Continuité des Opérations

Plan de communication de crise : canaux de contact alternatifs en cas de panne (numéros d'urgence, plateformes de messagerie externe)

Sites de repli pour les employés critiques

Fournisseurs alternatifs pour l'achat de bases de données médicales en cas d'interruption d'approvisionnement

Mise en place d'un cloud externe pour accéder aux données essentielles

6. Plan de Test

6.1. Objectifs du Test

Vérifier l'efficacité des procédures de secours

Évaluer le temps de rétablissement des services critiques

Identifier les éventuelles failles et axes d'amélioration

6.2. Scénarios de Test

Simulation de panne électrique : tester le basculement vers les systèmes de secours

Attaque cybernétique simulée : évaluer la réaction des équipes de cybersécurité

Défaillance matérielle d'un serveur critique : tester la restauration des données

Simulation de sinistre physique : mise en œuvre du site de repli

Interruption du réseau : test de continuité des opérations via un accès distant

6.3. Méthodologie du Test

Organisation d'exercices trimestriels

Suivi des indicateurs clés de performance (temps de récupération, taux de succès des restaurations)

Retour d'expérience et mise à jour du plan de secours

7. Plan de Maintenance

7.1. Maintenance Préventive

Mises à jour régulières des logiciels et des systèmes d'exploitation

Tests de sauvegarde et restauration pour garantir l'intégrité des données

Contrôle des infrastructures (alimentation, climatisation, onduleurs) pour éviter les pannes matérielles

Surveillance du réseau avec des outils de monitoring (logs, alertes en temps réel)

Audit de cybersécurité annuel pour identifier et corriger les vulnérabilités

7.2. Maintenance Corrective

Intervention rapide en cas de panne matérielle ou logicielle

Correction des vulnérabilités détectées lors des tests et audits

Remplacement des équipements obsolètes pour éviter les interruptions

Mise en place de correctifs d'urgence en cas de cyberattaque

7.3. Gestion des Mises à Jour

Planification des mises à jour en dehors des heures de production pour limiter l'impact

Tests préalables en environnement de préproduction pour éviter les incompatibilités

Déploiement progressif des mises à jour pour surveiller les effets

8. Plan de Reprise d'Activité

8.1. Activation du Plan

Déclenchement par le Directeur des Services Informatiques (DSI)

Information immédiate des employés concernés

Communication avec les partenaires stratégiques et les autorités

8.2. Reprise Informatique

Restauration des données via les sauvegardes les plus récentes

Basculement vers les serveurs de secours

Vérification de l'intégrité des systèmes et contrôle des accès

8.3. Reprise des Opérations Commerciales

Accès prioritaire aux outils de gestion des visiteurs médicaux

Mise en place d'une cellule d'assistance pour les régions impactées

Communication proactive avec les professionnels de santé

9. Suivi et Amélioration Continue

Tests réguliers du plan de secours (exercices de simulation)

Audit annuel des mesures de sécurité et de reprise

Mise à jour régulière des contacts d'urgence et des procédures