Plan de Reprise Anti-Sinistre Informatique

IT MEA Politiques & Procedures

|  |  |  |  |
| --- | --- | --- | --- |
| **Division** | Customer Technology Service | **Procédure Réf** | ITSOP\_Plan\_de\_Reprise\_Anti\_Sinistre  \_Informatique \_01-00 |
| **Département** | Technologies de l’information | **Procédure Date** | 1 May 2020 |
| **Procédure** | Plan de Reprise Anti-Sinistre Informatique | **Procédure Ver** | 1.0 |
| **Soumis Par** | Clinton Govender |
| **Approuvé par** | Roger Tabbal |

Table de Matière

[1. Objectif 3](#_Toc50997688)

[2. Équipe d’Urgence 3](#_Toc50997689)

[2.1. L’équipe d'intervention d'Urgence 3](#_Toc50997690)

[2.2. L’équipe d'intervention Informatique 3](#_Toc50997691)

[3. Systèmes et Infrastructures Informatiques 5](#_Toc50997692)

[3.1. Documentation des Systèmes & Infrastructure Informatique 6](#_Toc50997693)

[4. Stratégie de la Sauvegarde 6](#_Toc50997694)

[4.1. Procédures de la sauvegarde 7](#_Toc50997695)

[5. Gestion des Risques 8](#_Toc50997696)

[5.1. L’évaluation des Risques 8](#_Toc50997697)

[6. Financier et Juridique 8](#_Toc50997698)

[6.1. Évaluation des dégâts 9](#_Toc50997699)

[7. Procédures de Récupération du Système 9](#_Toc50997700)

[7.1. Procédures de Récupération Générales 10](#_Toc50997701)

[7.2. Procédures de Récupération des Systèmes Centralisés 10](#_Toc50997701)

[8. La Reprise après le Désastre 10](#_Toc50997702)

[8.1. Récupération des Processus Opérationnels 10](#_Toc50997703)

[9. Test et Revue du Plan de Récupération 11](#_Toc50997704)

# 1. Objectif

Le plan de reprise après un désastre détaille la procédure et les processus permettant aux  hôtels de se remettre aussi rapidement et efficacement que possible de toute urgence qui perturbe les systèmes d'information et les opérations. Le plan de récupération vise à minimiser

l'impact sur l'organisation en cas de perte ou d'endommagement des ressources, telles que le matériel ou les données informatiques.

Exemple des catastrophes qui peuvent inclure, mais elles ne sont pas limitées à :

* Panne d'électricité, incendie ou dommages physiques aux bâtiments
* Instabilité économique et politique
* Catastrophes naturelles telles que tremblements de terre, inondations et épidémies
* Guerre, terrorisme et troubles civils

# 2. Équipe d’Urgence

L'équipe d'intervention d'urgence et l'équipe de récupération sont composées de personnes internes et externes chargées d'exécuter, de maintenir et de tester le plan de récupération après un désastre.

## 2.1. l’Équipe d'intervention d'urgence

L'équipe d'intervention d'urgence est composée des personnes spécifiques internes qui sont responsables de la gestion globale du plan de reprise après un désastre.

|  |  |
| --- | --- |
| 2.1.1L’équipe d’intervention d’urgence – Rôles & responsabilités | Détails des contacts |
| * L'équipe d'intervention d'urgence assume la responsabilité globale de tous les incidents ayant un impact sur l’opération de l’hôtel.   Les fonctions de l’équipe d’urgence sont :   * + Réagir immédiatement à une catastrophe potentielle.   + Évaluer l'ampleur de la catastrophe et son impact potentiel sur les activités de l’hôtel.   + Décider quels éléments du plan de reprise doit être activés.   + Mettre en place et gérer les équipes de reprise appropriées.   + Assurer la communication avec tous les concernées de la situation actuelle et suivre l'avancement des taches du plan de reprise. |  |

## 2.2. l’Équipe d’intervention informatique

Comme indiqué ci-dessous, il y a trois équipes informatiques spécifiques. Les équipes sont composées de personnes spécialisées dans un domaine particulier et ils sont chargés d'exécuter des parties spécifiques du plan de reprise après un désastre.

Selon les circonstances, il n'est pas nécessaire d'activer toutes les équipes.

|  |  |
| --- | --- |
| 2.2.1 L’équipe d’intervention du réseau - Rôles & responsabilités | Détails des contacts |
| * L’équipe du réseau participe à la reprise des activités après le désastre, selon les instructions de l’équipe d’intervention d’urgence. * L’équipe du réseau évalue l'ampleur du désastre et l’impact sur l'ensemble de l'infrastructure réseau.   + L'infrastructure réseau comprend : les commutateurs (switches), les routeurs, le câblage, les points d'accès Wi-Fi, les salles de serveurs et les locaux techniques (IDF), le réseau WAN, les lignes internet et la téléphonie. * L’équipe du réseau établit un décompte des quantités et des coûts en fonction de l'évaluation des dégâts. * L’équipe du réseau élabore un plan d'action, en collaboration avec l’équipe d’intervention d’urgence, pour restaurer les services touchés. * L’équipe du réseau participe à la mise en place, à l'installation et à la configuration des services réseau afin de le remettre en état de fonctionnement normal, en respectant les normes Accor. * L’équipe du réseau collabore étroitement avec les équipes régionales de Accor afin de respecter les normes de Accor * L’équipe réseau partage un feedback précis et régulier avec l’équipe d’intervention d’urgence sur les activités qui relèvent de leur responsabilité. * L’équipe réseau fournit toute assistance requise par l’équipe d’intervention d’urgence. |  |

|  |  |  |
| --- | --- | --- |
| 2.2.2 L’équipe d’intervention des serveurs - Rôles & responsabilités |  | |
| * L’équipe d’intervention des serveurs participe à la reprise des activités après le désastre, selon les instructions de l’équipe d’intervention d’urgence. * L’équipe du réseau évalue l'ampleur du désastre et l’impact sur l'ensemble de l'infrastructure des serveurs.   + L'infrastructure des serveurs comprend : les serveurs physiques, les serveurs virtuels, l'installation du système d'exploitation, la préparation de l'installation des applications, les racks et le câblage des serveurs. * L’équipe d’intervention des serveurs établit un décompte des quantités et des coûts en fonction de l'évaluation des dégâts. * L’équipe d’intervention des serveurs élabore un plan d'action, en collaboration avec l’équipe d’intervention d’urgence, pour restaurer les services touchés. * L’équipe d’intervention des serveurs participe à la mise en place, à l'installation et à la configuration des services réseau afin de le remettre en état de fonctionnement normal, en respectant les normes Accor. * L’équipe d’intervention des serveurs collabore étroitement avec les équipes régionales de Accor afin de respecter les normes de Accor * L’équipe d’intervention des serveurs partage un feedback précis et régulier avec l’équipe d’intervention d’urgence sur les activités qui relèvent de leur responsabilité. * L’équipe d’intervention des serveurs fournit toute assistance requise par l’équipe d’intervention d’urgence. |  | |
| 2.2.3 L’équipe d’intervention des applications - Rôles & responsabilités | |  |
| * L’équipe d’intervention des applications participe à la reprise des activités après le désastre, selon les instructions de l’équipe d’intervention d’urgence. * L'équipe d’intervention des applications évalue l'ampleur du désastre et son impact sur les applications.   + Les applications comprennent, le PMS, le POS, les applications financières, les applications de la gestion des ressources humaines RH, les serrures de portes, l'IPTV… * L’équipe d’intervention des applications établit un décompte des quantités et des coûts en fonction de l'évaluation des dégâts. * L’équipe d’intervention des applications élabore un plan d'action, en collaboration avec l’équipe d’intervention d’urgence, pour restaurer les services touchés. * L’équipe d’intervention des applications participe à la mise en place, à l'installation et à la configuration des services réseau afin de le remettre en état de fonctionnement normal, en respectant les normes Accor. * L’équipe d’intervention des applications collabore étroitement avec les équipes régionales de Accor afin de respecter les normes de Accor * L’équipe d’intervention des applications partage un feedback précis et régulier avec l’équipe d’intervention d’urgence sur les activités qui relèvent de leur responsabilité. * L’équipe d’intervention des applications fournit toute assistance requise par l’équipe d’intervention d’urgence. | |  |

# 3. Systèmes & Infrastructure Informatiques

Tous les systèmes et infrastructures informatiques utilisés à l'hôtel doivent être documentés de manière aussi précise que possible. Ces documents permettront à l’équipe d’intervention d’urgence et aux équipes de récupération de se remettre du désastre le plus rapidement possible.

Les documents et processus suivants doivent être en place :

* Un inventaire complet et à jour du matériel et des logiciels (y compris les licences). L'inventaire du matériel et des logiciels doit être vérifié et signé par le responsable informatique chaque trimestre.
* Un document complet et à jour sur le réseau doit être maintenu, comprenant tous les détails sur les équipements de réseau, les diagrammes, la configuration, les détails de sécurité, etc.
* Un document complet et à jour sur les systèmes doit être maintenu, comprenant toutes les versions, les diagrammes, la configuration, les détails de sécurité, etc.
* Les documents doivent être stockés en toute sécurité, à la fois sur papier et sur support électronique (sur un système de stockage en nuage approuvé par l'entreprise), et ne doivent être accessibles qu'à l'IT et le GM.
* Tous les documents doivent être révisés au moins une fois par an ou à chaque fois qu'un changement majeur survient dans l’hôtel.

## 3.1. Documentation des Systemes & Infrastructure informatique

|  |  |
| --- | --- |
| 3.1.1 Inventaire des matériels | Document |
| Veuillez insérer ici le document d'inventaire du matériel de votre hôtel. Veuillez-vous assurer que toutes les directives ci-dessus sont respectées. L'inventaire du matériel peut également être un document individuel ou une partie du document d'infrastructure informatique. | **Insérer Document** |
| 3.1.2 Inventaire des logiciels | Document |
| Veuillez insérer ici le document d'inventaire des logiciels de votre hôtel. Veuillez-vous assurer que toutes les directives ci-dessus sont respectées. L'inventaire des logiciels peut également être un document individuel ou une partie du document d'infrastructure informatique | **Insérer Document** |
| 3.1.3 Documentation du réseau | Document |
| Veuillez insérer ici le document de réseau de votre hôtel. Veuillez-vous assurer que toutes les directives ci-dessus sont respectées. Le document de réseau peut également être un document individuel ou une partie du document d'infrastructure informatique. | **Insérer Document** |
| 3.1.4 Documentation des systèmes | Document |
| Veuillez insérer ici la documentation du système de votre hôtel. Veuillez-vous assurer que toutes les directives ci-dessus sont respectées. La documentation du système peut également être un document individuel ou une partie du document d'infrastructure informatique. | **Insérer Document** |

# 4. Stratégie de la Sauvegarde

En cas d'un désastre, la clé de la reprise est de disposer d'une sauvegarde intégrale. Il est essentiel de mettre en place une stratégie de sauvegarde complète et sûre qui vous permette de vous remettre de n'importe quel désastre pour n'importe quel système.

La stratégie de sauvegarde complète doit garantir :

* Les procédures de sauvegarde pour chaque système doivent être documentées.
* .
* Les journaux de sauvegarde sont vérifiés et signés quotidiennement, puis stockés en toute sécurité sur papier et sur support électronique (sur un stockage en cloud approuvé par Accor). Cela doit également inclure les journaux des tâches de script d'exportation de sauvegarde, si applicable.
* Les journaux de sauvegarde sont disponibles pour un minimum des 90 derniers jours pour toutes les sauvegardes.
* Les sauvegardes sont maintenues dans la structure fils, père et grand-père.
* Des supports de sauvegarde primaires et secondaires sont utilisés.
* Un test de restauration des fichiers de sauvegarde de tous les systèmes critiques est effectué une fois par trimestre.
* Un test de restauration des fichiers de sauvegarde pour tous les systèmes non critiques est effectué une fois tous les six mois.
* Les résultats des tests de restauration sont documentés et signés par le responsable informatique, puis stockés en toute sécurité sur papier et sur support électronique (sur un stockage en cloud approuvé par Accor).
* Une maintenance adéquate des équipements et des supports de sauvegarde doit être assurée, y compris le cycle de vie des supports de sauvegarde, l'utilisation de supports de nettoyage, etc…
* Le logiciel de sauvegarde utilisé doit être supporté par un contrat d'assistance en vigueur.
* Tous les utilisateurs doivent stocker leurs données professionnelles sur le serveur ou sur un stockage en cloud (SharePoint) approuvé par Accor.

En revanche, les procédures ci-dessous doivent être respectées pour les sauvegardes sur site :

* Tous les supports de sauvegarde sont clairement étiquetés et stockés dans un endroit sûr.
* Au moins deux (02) séries de sauvegardes hebdomadaires tournantes sont en place.
* Les supports de sauvegarde sont placés dans un coffre-fort antifeu immédiatement après la sauvegarde.
* Le coffre-fort antifeu doit être situé à l'écart des salles de serveurs et l'accès a ce dernier doit être limité à l'IT et au GM.
* Les supports de sauvegarde hebdomadaires, mensuels et annuels doivent être stockés dans un lieu sécurisé hors site, à quatre (04) heures maximums de l'hôtel.
* Un registre des supports de sauvegarde est maintenu pour suivre le stockage de tous les supports de sauvegarde.

Pour la sauvegarde en cloud, il est recommandé de mettre en œuvre la solution régionale de sauvegarde en cloud (Barracuda) et de la configurer conformément aux standards Accor.

## 4.1. ProcÉdures de la sauvegarde

|  |  |
| --- | --- |
| 4.1.1 Sauvegarde Barracuda en Cloud | Document |
| La procédure ci-jointe doit être suivie pour : configurer, sauvegarder et restaurer les données en utilisant la solution Barracuda cloud backup. |  |
| 4.1.2 Sauvegarde sur site | Document |
| Si l’hôtel dispose de sa propre solution de sauvegarde sur site, la procédure ci-jointe doit être suivie pour : configurer, sauvegarder et restaurer les données conformément aux normes Accor. | **Insérer Document** |
| 4.1.3 La liste de vérification de la sauvegarde des applications | Document |
| Veuillez compléter la liste de contrôle ci-jointe avec les détails de sauvegarde de tous les systèmes.  Prière d’ajouter des systèmes supplémentaires qui ne figurent pas dans la liste. |  |

# 5. Gestion des Risques

Il y a des nombreuses menaces potentielles qui peuvent affecter les activités normales d'un hôtel. Une évaluation des risques permet d'identifier les dangers pour l’hôtel et d'évaluer la probabilité d'un incident et son impact. Le fait de pouvoir identifier ces risques permet également à l’hôtel de mettre en œuvre les mesures de réduction des risques afin de minimiser l'impact ou de le neutraliser complètement.

## 5.1. L'ÉVALUATION DES RISQUES

|  |  |
| --- | --- |
| 5.1 L’évaluation des risques |  |
| Veuillez remplir le formulaire d'évaluation des risques ci-joint en respectant les étapes suivantes :   * Identification des risques importants qui peuvent affecter l’hôtel. * Classification de chaque risque en fonction de sa fréquence d'apparition. * Évaluation de chaque risque en fonction de son impact possible sur l’hôtel. * Prévoir les mesures potentielles de réduction ou d'atténuation des risques. |  |

***Financier et Juridique***

L'équipe d'intervention d'urgence coopère avec les autres équipes d'intervention pour préparer une évaluation initiale de l'impact de l'incident sur les affaires financières de l’hôtel. Cette évaluation doit comprendre les éléments suivants :

* La perte de matériel informatique
* La perte de logiciels
* La perte de matériel de télécommunication
* Dégâts aux infrastructures et aux bâtiments

Dans le cadre des stratégies de l'entreprise en matière de désastre, de reprise de l’activité et de continuité des services à l’hôtel, des assurances doivent être en place. Celles-ci comprennent les erreurs et les oublis, la responsabilité des administrateurs et des dirigeants, la responsabilité civile générale et l'assurance contre les pertes d'exploitation.

Le service juridique de l'entreprise et l'équipe d’intervention d'urgence examineront ensemble les conséquences de l'incident et décident s'il peut y avoir des actions juridiques à la suite de la catastrophe ; en particulier, la possibilité de réclamations par ou contre l’hôtel pour des violations de la réglementation, etc...

## 6.1. ÉVALUATION DES dÉgÂts

|  |  |  |
| --- | --- | --- |
| 6.1 | L’évaluation des dégâts |  |
|  | Après un incident, il faudra remplir un formulaire d'évaluation les dégâts pour justifier : une réclamation d'assurance, une action en justice et pour justifier les coûts de remplacement. |  |

***Procédures de Récupération du Système***

Les procédures de restauration du système détaillent les étapes nécessaires pour rétablir un système dans son état opérationnel requis.

|  |
| --- |
| 7.1 Procédures de récupération générales |
| 1. Informez l’équipe d’intervention d’urgence de la situation. 2. Ouvrez un ticket MyIT en envoyant un courriel à [MyIT@accor.com](mailto:MyIT@accor.com). 3. Informer le Directeur Informatique du Pays ou le Cluster de la situation. 4. Exécuter le plan d’urgence (PMS, POS) pour les systèmes affectés. 5. Contactez les équipes d’interventions requises. 6. Évaluer la situation avec les différentes équipes d’interventions et informer l’équipe d’intervention d’urgence des résultats. 7. Établir un plan d'action avec l’autorisation de l’équipe d’intervention d’urgence. 8. Prendre des mesures temporaires pour rendre les opérations fonctionnelles dès que possible. 9. Fournir le matériel et les logiciels nécessaires conformément au plan d'action. 10. Installer et configurer le matériel et les logiciels conformément au plan d'action. 11. Restaurer les systèmes avec la dernière bonne sauvegarde et configuration. 12. Effectuer des tests d'acceptation par l'utilisateur pour s'assurer que tous les systèmes sont opérationnels comme prévu. 13. Remise en services des systèmes. 14. Mener une analyse approfondie du processus de reprise après désastre et documenter les résultats. 15. Mettre à jour le plan de reprise après le désastre en conséquence. 16. Assurer une communication claire et cohérente avec toutes les parties concernées tout au long du processus. |

## 7.2. PROCÉDURES DE RÉCUPÉRATION Des SYSTÈMEs CENTRALisÉs

|  |  |
| --- | --- |
| * 1. Procédures de récupération des systèmes centralisés |  |
| * + 1. Utilisez la procédure suivante pour installer et configurer Opera sur site V5.5.0.26 sur W2K12 R2   Cette procédure peut également être utilisée pour l'installation de la version cloud. |  |
| 7.2.2 Utilisez la procédure suivante pour installer et configurer Simphony  Cette procédure peut également être utilisée pour l'installation de la version cloud. |  |

***La Reprise après le Désastre***

Une fois les opérations sont rétablies, il sera nécessaire de rendre la direction des opérations spécifiques aux responsables concernés. Il est probable que, pendant le processus de rétablissement, la responsabilité globale ait été attribuée à l’équipe d’intervention d’urgence et aux différentes équipes d’intervention. Une fois le rétablissement terminé, le processus doit être formalisé afin de s'assurer que toutes les parties comprennent le changement de responsabilité globale et le retour à la normale.

## 8.1. RÉcupÉration des Processus OpÉrationnels

|  |  |
| --- | --- |
| 8.1 Récupération des Processus Opérationnels |  |
| Le formulaire de clôture de la récupération doit être signé par le chef de l'équipe de récupération et par le responsable du département concerné pour chaque processus qui a été récupéré et remis aux opérations avec succès. |  |

# Test et Revue du Plan de Récupération

Le test du plan de reprise après un désastre est une partie essentielle du processus d'élaboration du plan. L'exercice de test est conçu comme une expérience d'apprentissage : l'objectif est de comprendre ce qui doit être amélioré et comment les améliorations peuvent être mises en œuvre.

Le test du plan permet de s'assurer que les équipes d'urgence connaissent bien leurs missions et, surtout, qu'elles ont confiance en leurs capacités. Ce plan de reprise après sinistre doit être testé et révisé au moins une fois par an.