SYNITEL
INFORMATIQUE
Sarl au capital de : 38112.25€ - SIRET : 353 326 556 00019 APE : 723Z
N° identification TVA : FR55 35332655600019
24, Chemin du Marais - 73420 VOGLANS
Téléphone : 04.79.88.60.60 - Fax : 04.79.88.60.61
Email : contact@synitel.com - Internet : www.synitel.com

PLAN DE CONTINUITE

D'ACTIVITE

PCA

SOMMAIRE

1. Objectif

En informatique, un plan de continuité d'activité, a pour but de garantir la survie de l'entreprise après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise.

2. Étapes de la mise en place d'un plan de continuité

2.1. Analyse de risque et d'impact

Pour qu'un plan de continuité soit réellement adapté aux exigences de l'entreprise, il doit reposer sur une analyse de risque et une analyse d'impact :

• L'analyse de risque débute par une identification des menaces sur l'informatique. Les menaces peuvent être d'origine humaine (attaque délibérée ou maladresse) ou d'origine « naturelle »; elles peuvent être internes à l'entreprise ou externes. On déduit ensuite le risque qui découle des menaces identifiées; on mesure l'impact possible de ces risques. Enfin, on décide de mettre en œuvre des mesures d'atténuation des risques en se concentrant sur ceux qui ont un impact significatif. Par exemple, si le risque de panne d'un équipement risque de tout paralyser, on installe un équipement redondant. Les mesures d'atténuation de risque qui sont mises en œuvre diminuent le niveau de risque, mais elles ne l'annulent pas: il subsiste toujours un risque résiduel, qui sera couvert soit par le plan de continuité, soit par d'autres moyens (assurance, voire acceptation du risque)

• L'analyse d'impact consiste à évaluer quel est l'impact d'un risque qui se matérialise et à déterminer à partir de quand cet impact est intolérable, généralement parce qu'il met en danger les processus essentiels (donc, la survie) de l'entreprise. L'analyse d'impact se fait sur base de désastres: on considère des désastres extrêmes, voire improbables (par exemple, la destruction totale du bâtiment) et on détermine les impacts financiers, humains, légaux, etc., pour des durées d'interruption de plus en plus longues jusqu'à ce qu'on atteigne l'impact maximal tolérable. Le résultat principal de l'analyse d'impact est donc une donnée temporelle: c'est la durée maximale admissible d'une interruption de chaque processus de l'entreprise. En tenant compte des ressources informatiques (réseaux, serveurs, PCs…) dont chaque processus dépend, on peut en déduire le temps maximal d'indisponibilité de chacune de ces ressources, en d'autres termes, le temps maximal après lequel une ressource informatique doit avoir été remise en fonction. Une analyse de risque réussie est le résultat d'une action collective impliquant tous les acteurs du système d'information : techniciens, utilisateurs et managers.

2.2. Choix de la stratégie de sécurisation

Il existe plusieurs méthodes pour assurer la continuité de service d'un système d'information. Certaines sont techniques (choix des outils, méthodes de protection d'accès et de sauvegarde des données), d'autres reposent sur le comportement individuel des utilisateurs (extinction des postes informatiques après usage, utilisation raisonnable des capacités de transfert d'informations, respect des mesures de sécurité), sur des règles et connaissances collectives (protection incendie, sécurité d'accès aux locaux, connaissance de l'organisation informatique interne de l'entreprise) et de plus en plus sur des conventions passées avec des prestataires (copie des programmes, mise à disposition de matériel de secours, assistance au dépannage).
Les méthodes se distinguent entre préventives (éviter la discontinuité) et curatives (rétablir la continuité après un sinistre). Les méthodes préventives sont souvent privilégiées, mais décrire les méthodes curatives est une nécessité car aucun système n'est fiable à 100 %.

3. Mesures préventives

Besoin des solutions suivantes afin d'assurer la continuité de service de leurs applications métiers et infrastructures informatiques et télécoms sous-jacentes :

- Sauvegarde et restauration de données.
- Planning des actions à mener en cas de crise.
- Conservation et archivage de données.

Viennent ensuite, par ordre décroissant de citations, les solutions de réplication, mirroring, Agrégat par bandes et secours multi-sites ou sur un autre site distant, de basculement sur un réseau de secours, d'analyse de procédures et stratégies assurant la continuité de business, de gestion de bande passante, de sécurité physique et logique …

3.1. La sauvegarde des données

La préservation des données passe par des copies de sauvegarde régulières. Il est important de ne pas stocker ces copies de sauvegarde à côté du matériel informatique, voire dans la même pièce car elles disparaitraient en même temps que les données à sauvegarder en cas d'incendie, de dégât des eaux, de vol, etc. Lorsqu'il est probable que les sauvegardes disparaissent avec le matériel, le stockage des copies de sauvegarde peut alors être nécessaire dans un autre lieu différent et distant. L'analyse d'impact a fourni des exigences exprimées en temps maximal de rétablissement des ressources après un désastre (RTO Recovery Time Objective) et la perte maximale de données (Recovery Point Objective). La stratégie doit garantir que ces exigences seront observées. C'est pour cela que la solution de sauvegarde en ligne vient en complément d'une sauvegarde sur bandes.

3.2. Les systèmes de secours

Il s'agit de disposer d'un système informatique équivalent à celui pour lequel on veut limiter l'indisponibilité : ordinateurs, périphériques, systèmes d'exploitation, programmes particuliers, etc. Une des solutions consiste à créer et maintenir un site de secours, contenant un système en ordre de marche capable de prendre le relais du système défaillant. Selon que le système de secours sera implanté sur le site d'exploitation ou sur un lieu géographiquement différent, on parlera d'un secours in situ ou d'un secours déporté.

4. Mesures curatives

Selon la gravité du sinistre et la criticité du système en panne, les mesures de rétablissement seront différentes.

4.1. La reprise des données

Dans cette hypothèse, seules des données ont été perdues. L'utilisation des sauvegardes sur bandes est nécessaire et la méthode, pour simplifier, consiste à réimplanter le dernier jeu de sauvegardes. Cela peut se faire dans un laps de temps court, si l'on a bien identifié les données à reprendre.

4.2. Le redémarrage des applications

A un seuil de pannes plus importantes, une ou des applications sont indisponibles. A restauration du système sera une solution à envisager, voir l'utilisation d'un site de secours, le temps de rendre disponible l'application en cause

4.3. La perte totale du système informatique

La seule solution est l'utilisation d'un site de secours le temps du remplacement du système.

5. Moyens mis en œuvre

5.1. Prérequis

- Votre système informatique doit être à jour (mises a jour système d'exploitation, logiciels antivirus etc.) et les sauvegardes valides
- Dans le cas d'un serveur avec domaine les postes clients doivent se connecter en bureau à distance (RDP) afin de pouvoir basculer sur un serveur distant temporaire.
- Une sauvegarde en ligne des données critiques (dernière année en gestion, comptabilité etc.) doit être disponible et valide

5.2. Sauvegarde

• La société SYNITEL vous propose une sauvegarde en ligne délocalisée Oodrive qui permet la récupération des données nécessaire à la continuité de votre activité
• En complément de la sauvegarde en ligne nous installons une sauvegarde sur bande, disque externe ou NAS avec le logiciel BackupAssist. Cette sauvegarde de vos applications de gestion s'effectue tous les jours et permet de palier à une perte de donnée sensible.
• Nous mettons en place une sauvegarde hebdomadaire sur dique dur externe qui permet de sauvegarder toute vos données y compris les données des utilisateurs (courrier, photos etc.)

5.3. Système de secours

Pour répondre aux problématiques de recouvrement de désastre, la société SYNITEL dispose de serveurs de secours qui permettent à votre société de pouvoir redescendre votre sauvegarde Oodrive sur un serveur temporaire préconfiguré avec vos principales applications de gestion.

6. Intervention type

•Le cabinet EXPERTISE AUTOMOBILE utilise le logiciel Expert Office sur un serveur avec domaine situé dans ses locaux et tous les postes informatiques sont connectés sur ce serveur en bureau à distance.
Les données de gestion des trois dernières années ainsi que la configuration du logiciel métier sont sauvegardées en ligne toutes les nuits.
En complément une sauvegarde journalière sur un NAS situé sur site est effectuée.
Une sauvegarde complète hebdomadaire sur deux disques externes en rotation (la dernière sauvegarde hebdomadaire est conservée hors site) se déclenche chaque week-end.

•Suite à un incendie le système informatique est totalement détruit.

•La société SYNITEL dispose dans ses locaux de serveurs de secours ou est installé une configuration opérationnelle du logiciel Expert Office. Dès l'appel du cabinet nous restaurons la sauvegarde en ligne du cabinet sur un de ces serveurs.
Nous communiquons l'adresse de connexion ou, si les locaux sont toujours utilisables, nous installons le serveur de secours sur site afin que les utilisateurs puissent depuis n'importe quel poste informatique se connecter grâce au bureau à distance.
Les dossiers du cabinet peuvent continuer à être traités le temps de réinstaller un nouveau système complet sur le nouveau site de l'entreprise.
L'intégralité des données sauvegardées seront récupérées sur le nouveau système informatique.

Notre partenariat avec la société SIDEXA nous permet de gérer intégralement ces processus sans passer par d'autres intervenants. Cela permet de simplifier et accélérer la reprise de votre activité.