



POUR MAITRISER LES RISQUES DANS VOS ACTIVITES IL FAUT TOUJOURS AVOIR UN BON PLAN ... DE SAUVEGARDE

La pratique des sauvegardes est entrée dans les habitudes professionnelles.

La pratique ... oui, par contre, la gestion, une gestion dûment formalisée à partir d'une analyse des besoins et de modalités préalablement définis, c'est autre chose !

Et pourtant, ...

DES SAUVEGARDES, SINON ...

Il n'existe pas d'alternative. Une duplication régulière des ressources informationnelles vitales de l'entreprise est la seule parade contre les risques d'indisponibilité, de dégradation ou de perte de celles-ci.

Cette opération doit donc s'inscrire au premier rang dans les conditions de réalisation d'un plan de continuité d'activité

Et la taille de l'entreprise ne fait rien à l'affaire.

DANS LE CADRE D'UN PLAN DE SAUVEGARDE, SINON ...

Perte, vol, oubli, dysfonctionnement, non-conformité ... des menaces spécifiques nombreuses pèsent sur la gestion des sauvegardes.

Elles doivent être traitées dans une instruction dédiée, un plan de sauvegarde.

Et plus, ce plan doit, non seulement exister, mais il doit être complet. Il doit comprendre toutes les mesures de sécurité et toutes les règles de gestion destinées à traiter l'ensemble des risques associés à la démarche, et ils sont nombreux.

ET POURTANT ...

Cette démarche de formalisation, indispensable à la sécurité des transactions, est encore, trop souvent, négligée, desservie par une certitude reçue et resservie régulièrement :

"Les sauvegardes sont faites ! Ça marche ! Il n'y a pas de problème, alors pourquoi vouloir rédiger une instruction de plus ? Il y a mieux à faire que d'écrire ce que l'on fait correctement depuis longtemps !"

Combien de fois sommes-nous confrontés à cette incompréhension pour des démarches de sécurité pourtant essentielles, mais perçues comme l'expression d'un abus de formalisme.

Il faut donc, dans ce domaine aussi, convaincre bon nombre d'interlocuteurs, tant stratégiques que fonctionnels et opérationnels, de la nécessité de **DISPOSER D'UN PLAN DE SAUVEGARDE COMPLET, A JOUR** mais aussi **REGULIEREMENT TESTE**, nous y reviendrons.

... C'EST UNE DEMARCHE STRATEGIQUE

Objectifs, moyens, solutions, données protégées ... la politique de sauvegarde à l'origine du plan est une démarche de direction par les enjeux servis et les arbitrages exigés à partir des éléments proposés à l'étude et à la décision par les partenaires à la maîtrise d'œuvre sécurité de l'information (voir l'article "[Définir les rôles et les responsabilités](#)" sur ce site).

MAIS, TOUT D'ABORD, LES LIMITES DE CET ARTICLE

Sauvegarde incrémentale ou sauvegarde complète, solution centralisée, automatisée, solutions extérieures ... vous ne trouverez pas dans l'article de recommandations techniques sur les modalités de sauvegarde. Ce n'est pas son objet; son objet c'est de proposer à la réflexion des éléments utiles à l'approche managériale de cet acte majeur de prévention / protection.

Ça ne veut pas dire, pour autant, qu'il n'intéresse pas les gestionnaires informatiques, bien au contraire.

Ceux-ci sont, en effet, doublement intéressés par la démarche. Ils le sont à la fois en tant que fournisseurs de services informatiques auprès des métiers, mais ils le sont aussi en tant que responsables de ressources vitales du système d'information de l'entreprise, des ressources qu'il convient de sauvegarder également de la façon la plus sûre.

Ça ne veut pas dire non plus qu'il n'intéresse pas ceux qui ont déjà leur plan.

En effet, pourquoi ne pas vérifier si, après tout, le compte y est bien, car, nous le savons, le risque de dénaturation des actions répétitives s'accroît naturellement avec le temps.

Ceci posé, l'objet de l'article est d'établir, autant que possible, l'inventaire des sujets à traiter dans un plan de sauvegarde pour ne rien oublier.

Pour servir cet objectif, le document est globalement structuré autour des principales rubriques que l'on ne doit pas manquer d'examiner lors de la rédaction du plan.

L'article est basé sur un retour d'expérience personnel.

Aussi souffre-t-il certainement de manques et d'approximations. Ne manquez pas de les faire connaître à son auteur afin de garantir à sa proposition d'information le meilleur niveau possible.

LE PLAN DE SAUVEGARDE SOUSCRIT AUX REGLES JURIDIQUES APPLICABLES

En effet, lors de l'élaboration du plan de sauvegarde, non seulement il convient de tenir compte des obligations juridiques générales (protection des données à caractère personnel), mais aussi des réglementations spécifiques éventuellement applicables dans votre domaine d'activité (contrôle interne, sécurité financière, certification des comptes, données de santé ...)

LE PLAN DE SAUVEGARDE FAIT L'INVENTAIRE DE TOUTES LES RESSOURCES SENSIBLES DE L'ENTREPRISE

La politique de sauvegarde ne concerne pas que les données de gestion, de ressources humaines, les informations comptables et financières ou autres.

Elle s'applique à toutes les ressources informationnelles critiques de l'entreprise, les ressources informatiques (système d'exploitation, applications ...) mais aussi les ressources de télécommunication et d'autres comme, par exemple, des moyens de pilotage automatisés ...

Par contre, toutes les ressources ne sont pas à sauvegarder. Lourdeur des opérations, aggravation des risques de dysfonctionnement, charges financières, ce serait contre-productif d'avoir cette ambition, sauf si la totalité des actifs d'information détenus et gérés par l'entreprise le justifie par leur niveau de sensibilité.

Il faut donc commencer par identifier, de façon exhaustive, les données à protéger par l'évaluation de l'impact de leur manque sur l'activité et l'image de marque de l'organisation.

C'est pourquoi, la définition d'une politique de sauvegarde impose d'établir le niveau de sensibilité du patrimoine informationnel de l'entreprise afin de répondre à ses besoins essentiels d'activité, et de déterminer les moyens de protection les mieux adaptés aux différents composants de ce patrimoine.

LE PLAN DE SAUVEGARDE NE DOIT PAS CONFONDRE ARCHIVAGE ET SAUVEGARDE

L'archivage d'informations définitivement figées, mais dont la conservation s'impose dans la durée, ne doit pas être assimilé aux sauvegardes de données et de ressources primaires vivantes. Ces informations souscrivent à des solutions de conservation spécifiques.

Cette distinction ne dispense pas, bien sûr, d'en tenir un inventaire à jour, et d'évoquer leur traitement, de façon générale, dans le plan.

LE PLAN DE SAUVEGARDE N'OUBLIE PAS LES DONNEES DES UTILISATEUR

Ces données locales non structurées ne doivent pas être ignorées. Certaines, pas toutes non plus, revêtent un caractère vital pour leur détenteur.

Deux solutions sont possibles :

- soit, une solution d'administration globale, et les ressources importantes qu'elle peut exiger pour garantir une fiabilité délicate
- soit, l'initiative laissée aux utilisateurs, mais sous deux conditions :
 - mettre à leur disposition une solution de sauvegarde commode, un serveur partagé par exemple
 - assurer une communication de sensibilisation pédagogique, sur l'intérêt de sauvegarder régulièrement des données bureautiques professionnelles sensibles, des données qui, si elles venaient à manquer, pénaliseraient leur utilisateur.

APRES L'INVENTAIRE DES RESSOURCES CRITIQUES, LA PERIODICITE ET LA PLANIFICATION DES SAUVEGARDES

Une fois la réponse apportée à la question "Quelles données, quelles ressources me sont indispensables pour garantir le maintien de mon activité en cas de grandes difficultés ?", se posent deux autres questions déterminantes pour établir le plan de sauvegarde :

- Le délai d'interruption maximal admissible de l'activité, du service
- Le degré d'acceptabilité de perte de données sans préjudice grave dans le contexte d'un accident de sécurité majeur

En effet, quotidienne, bi quotidienne, hebdomadaire, mensuelle, à la demande, lors de mises à jour ... le rythme des sauvegardes est déterminé en fonction de l'intensité des mouvements de gestion à enregistrer et du niveau de criticité des données mouvementées, jusqu'à mettre en place une solution en temps réel¹ si le niveau de criticité des ressources l'exige.

C'est l'évaluation du degré de dépendance des activités aux ressources inventoriées qui fait la distinction entre :

- Les données non prioritaires
- Les données prioritaires, à rétablir dans des délais courts mais variables selon les besoins
- Les données dont vous avez besoin dans des conditions particulières notamment d'échéance (clôture de paie, exercice comptable ...)

Et, il est vrai que, dans ce cas, la multiplication de sauvegardes séparées facilite les restaurations en tant que de besoin et limite les risques de non récupération des données.

Par contre, il ne faut pas oublier de garantir une synchronisation absolue entre les sauvegardes. C'est pourquoi, une fois les fréquences déterminées, il convient également de définir les jours (ou les nuits) et les horaires des sauvegardes.

Et toutes ces informations, fréquences, jours, heures, sont précisées sur le plan pour chacune des ressources.

LE PLAN DE SAUVEGARDE EST UNE DEMARCHE COLLECTIVE

Pas de doute, dans cette démarche d'analyse des besoins, ce sont les métiers, les gestionnaires de processus, qui sont les mieux placés pour déterminer les exigences de sauvegarde indispensables à leurs activités.

Sur un plan général, la désignation indispensable d'un responsable de la tenue d'un plan de sauvegarde ne doit pas faire oublier que la démarche est collective. L'oubli de ce principe est souvent à l'origine des défauts, des défaillances d'organisation et de gestion constatés.

¹ Les répliquions en temps réel ne sont pas à l'abri de défaillance. Aussi cette solution ne dispense-t-elle pas de réaliser des sauvegardes régulières des données concernées.

LE PLAN DE SAUVEGARDE DONNE UNE DESCRIPTION PRECISE DES GESTIONS

Nous l'avons dit, le choix de la (des) solution(s) de sauvegarde appartient à la Direction à partir des travaux et des recommandations des partenaires à la gestion et l'utilisation des moyens concernés. Et ce choix dépend des contraintes d'activité, des exigences juridiques, des moyens, financiers, matériels, en personnel dont l'organisation dispose, mais également des besoins définis à partir de l'évaluation des pertes et délais d'interruption de service admissibles.

Naturellement, les principes et les options définis sont traduits en modalités de gestion, des modalités qui doivent être précisément décrites dans le plan de sauvegarde.

En effet, les informations portées dans l'instruction publiées représentent un engagement en responsabilité de la part de l'ensemble des intervenants et permettent d'assurer le suivi des actions.

Ainsi, de l'étiquetage des supports à leur conservation, en passant par les personnels habilités..., le plan de sauvegarde doit décrire les opérations générales et spécifiques à accomplir pour chaque ressource.

Il doit le faire sans tomber dans le détail superflu afin de préserver au plan de sauvegarde son caractère de document de référence, de document utilisable et opposable si une situation le justifie.

Nous ne développerons pas l'ensemble des éléments susceptibles d'être portés dans un plan de sauvegarde sous peine de tomber nous-mêmes dans le travers que nous dénonçons.

Mais, cependant, il nous paraît utile d'attirer l'attention sur quelques points particuliers.

LE PLAN DE SAUVEGARDE EVOQUE UN (DES) LIEU(X) DE STOCKAGE

Sauvegardes locales, duplications déposées régulièrement sur un site distant, il faut identifier un (des) lieu(x) de stockage des supports de sauvegarde, non seulement pour éviter leur oubli dans un lecteur ou sur le coin d'une table, mais également afin de garantir à la démarche les protections requises en matière de protection, de transport et d'habilitations à indiquer dans le plan, bien évidemment ...

Par contre, si le plan doit évoquer cette information, il doit le faire sans indiquer de coordonnées précises, pour des raisons élémentaires de confidentialité.

Et, ce lieu doit être épargné des risques d'incendie ou d'inondation. Le plus souvent c'est un coffre ignifugé, ou un local pour les grands centres, qui est préconisé.

UN PLAN DE SAUVEGARDE INTERNE COMPREND UN DISPOSITIF D'EXTERNALISATION PERIODIQUE DES RESSOURCES

Dans le cadre d'une solution de sauvegarde interne, l'externalisation, selon une périodicité à définir, d'une copie des sauvegardes sur un site distinct du site principal de conservation répond au risque d'indisponibilité de ce site dans l'éventualité d'un sinistre majeur.

Cette démarche doit particulièrement s'attacher à prendre en compte toutes les dispositions pour la protection des ressources, des dispositions présentées dans le plan (conditionnement, transports, habilitations, récupération ...).

Dans l'hypothèse où cette mise à l'abri d'une duplication des sauvegardes sur un site séparé utilise un service tiers, il faut contractualiser les engagements respectifs des partenaires hébergeur / hébergé (assurance, confidentialité, modalités d'accès, habilitations, responsabilités ...), et ce, qu'il s'agisse d'un service gratuit ou rémunéré.

LE PLAN DE SAUVEGARDE MENTIONNE UNE DATE DE VERSION ET LA NATURE DES MISES A JOUR

Il ne suffit pas de mettre en place une solution de sauvegarde expressément gérée, encore faut-il la mettre régulièrement à jour des évolutions de ses facteurs d'influence (applications, données, critères de sécurité, besoins ...)

Ainsi, le suivi des mises à jour nécessite l'indication dans le plan même des dernières modifications et de la date de sa version.

Cette information trouve naturellement sa place au côté de l'objet du document, de son degré de sensibilité (public), de son auteur et de son valideur dans son cartouche de présentation au titre d'une documentation de sécurité bien tenue.

LE PLAN DE SAUVEGARDE PREVOIT LES MODALITES DE VERIFICATION DU BON ACCOMPLISSEMENT DES OPERATIONS

Pour garantir, autant que possible, l'objectif servi, la restauration fiable, et dans les meilleurs délais, de données vitales pour l'entreprise, la procédure doit prévoir l'édition des résultats des opérations et les modalités de leur vérification.

Il s'agit d'une action de contrôle régulier indispensable, mais qui ne remplace pas les tests périodiques de lecture et de restauration des données qui s'imposent, des tests également à définir.

LE PLAN DE SAUVEGARDE PUBLIE LES REGLES DE MISE EN ŒUVRE DE TESTS PERIODIQUES DE RESTAURATION

Sauvegarder assidument les ressources inscrites au plan conformément aux modalités publiées, vérifier les journaux d'édition des opérations, c'est bien. Mais encore faut-il que ces sauvegardes soient exploitables le jour venu, un jour où l'obligation et l'urgence de résultats s'imposent.

Aussi, la politique et le plan de sauvegarde une fois définis, rédigés, publiés, il est indispensable de vérifier régulièrement la fiabilité des enregistrements. Il faut pour cela faire des tests de lecture et de restauration. Ceux-ci doivent être formellement prévus dans le plan avec toutes les indications utiles à leur suivi et leur évaluation (planification et traçabilité des opérations et de leurs résultats).

LES SOLUTIONS EXTERNALISEES DE SAUVEGARDE NE DISPENSENT PAS D'UN PLAN DE SAUVEGARDE

Avec le développement de l'informatique "dans les nuages", certains considèrent désormais que les sauvegardes locales appartiennent à une époque dépassée. Ce n'est pas si simple. Chaque solution comporte des avantages et des inconvénients en termes d'efficacité. Par conséquent le choix de l'externalisation aura fait l'objet d'une analyse et d'un arbitrage "Probabilité/Faisabilité/Impacts/Coûts", arbitrage tout ce qu'il y a de plus régulier en matière de protection de l'information.

Naturellement, le choix d'une solution de sauvegarde externalisée ne dispense pas de définir la politique et le plan de sauvegarde de l'entreprise.

Et plus, le choix de la sous-traitance impose aussi de considérer les risques spécifiques attachés à ce type de solutions de gestion.

En effet, le fournisseur d'une solution de gestion externalisée n'est pas épargné des risques de pertes de données et de rupture de service. Par conséquent, il lui appartient de prendre, et de justifier, de toutes les mesures de protection mises en œuvre pour s'en préserver.

Ainsi, le fournisseur d'une solution de sauvegarde externalisée appartient à ces "fournisseurs critiques" de l'entreprise évoqués par Robert BERGERON dans son article "[Les fournisseurs critiques](#)", des fournisseurs dont le rôle, comme il le rappelle, est souvent sous-estimé dans les dispositifs de continuité.

Par conséquent, nous ne saurions trop vous recommander la (re)lecture de l'information si vous avez à traiter une situation d'externalisation.

De même, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) publie ses recommandations en matière d'externalisation, notamment sur les obligations de continuité de service auxquelles le prestataire est assujéti, sur le plan de sauvegarde dont il doit justifier.

Mais pas seulement. Vous trouverez dans le document des informations utiles pour garantir les moyens de garder la maîtrise de ce type de solution, des informations sur le suivi des dispositions de sauvegarde et de continuité de l'hébergeur, mais aussi :

- La protection des données sensibles
- Le droit d'audit
- La réversibilité de la solution
- La propriété des informations
- La traçabilité des opérations ...

Son titre "[Maîtriser les risques de l'infogérance – Externalisation des Systèmes d'information](#)"

LE PLAN DE SAUVEGARDE EST NECESSAIRE AU CONTROLE INTERNE

La sauvegarde des actifs d'information répond au risque de pertes de données, notamment de données financières et comptables.

Par conséquent, un plan de sauvegarde est exigé par les autorités internes ou externes habilités à opérer les évaluations de conformité prévues en la matière.

LE PLAN DE SAUVEGARDE EST UN COMPOSANT ESSENTIEL DU PLAN DE CONTINUITE D'ACTIVITE

UN PLAN DE SAUVEGARDE REDIGE, COMPLET, PUBLIE ET A JOUR, SINON RIEN !

Les règles générales et particulières de sauvegarde pour chaque ressource vitale, les moyens utilisés, les fréquences, les supports, les procédures de marquage, les conditions de stockage et de récupération, les règles de restauration, les habilitations ... toutes ces actions doivent figurer dans le plan de sauvegarde pour qu'il réponde à l'objectif qui lui est assigné, la récupération d'informations vitales sur incident.

Avec l'aide de quelques tableaux récapitulatifs, cette obligation de formalisation ne doit pas dissuader d'établir ce référentiel. Il est indispensable à la continuité de service.

Il occupe, en effet, une place essentielle dans le plan de continuité d'activité de l'entreprise, notamment dans son plan de secours informatiques, mais également dans l'approche par métier et processus du P.C.A..

A VOTRE ECOUTE ET À VOTRE DISPOSITION

Notre contribution vaut pour la communauté intéressée au management de la sécurité de l'information et de plan de continuité d'activité à la condition de tenir compte de vos apports par vos observations et vos questions. Ne manquez pas de nous en faire part. ✉ guillet.lionel@gmail.com

LA PRESENTE ANNEXE ne reprend que quelques informations sommaires dont nous mesurons les limites.

Il convient de vous reporter à l'article en tant que de besoin pour toute précision, et, à défaut envoyez un message à son auteur, il est à votre écoute quillet.lionel@gmail.com.

POUR RESUMER

Un plan de sauvegarde doit être complet et précis, il doit être :

- personnalisé en fonction de l'organisation et de la solution mise en place pour protéger les ressources vitales identifiées
- suffisamment détaillé pour éviter les interprétations et pour être mis en œuvre immédiatement en cas d'incident ou de déclenchement du plan de continuité d'activité.

Il doit donc comprendre toutes les indications indispensables à une bonne organisation et une bonne gestion des sauvegardes, des indications qui font l'objet de la synthèse ci-dessous.

1. IDENTIFIER LE DOCUMENT

En préalable, dans un cadre réservé, le document doit être identifié pour son classement dans la documentation de référence de la Sécurité de l'Information et du P.C.A.

Nom du document –

Classification – Public < Le document est destiné à être publié tout en étant adressé aux gestionnaires intéressés >

Liste des destinataires

N. de version – Date – Nature des mises à jour – Historique des mises à jour

Autorités responsables - <Directeur– Rédacteur– Valideur>

2. RAPPELER L'OBJET DE LA DEMARCHE – POURQUOI UN PLAN DE SAUVEGARDE ?

Formuler la problématique de sécurité posée

Les risques d'indisponibilité, de perte d'intégrité, d'interruption de service.

La gestion du plan de continuité de service de l'entreprise

Le respect d'engagements d'activité et les enjeux métier

Les obligations juridiques ...

Donner la solution, faire des copies régulières des ressources informationnelles critiques pour les activités de l'entreprise

Faire valoir L'objectif poursuivi, répondre à deux situations :

- Pouvoir récupérer, le plus rapidement possible, une information
- Etre capable, en cas de perte totale, de reconstituer un environnement informationnel identique.

Formaliser, publier les règles et les modalités de gestion précises à respecter pour garantir la fiabilité de cette action essentielle, définir, publier, gérer le plan de sauvegarde de l'entreprise.

DEFINIR LE PERIMETRE DU PLAN DE SAUVEGARDE

Les ressources inscrites au plan de sauvegarde, ressources informatiques, programmes, environnements systèmes, environnements d'exploitation, données applicatives, données locales ...

3. IDENTIFIER L'INSTANCE CHARGÉE DE LA CONSERVATION ET DE LA RESTAURATION DES LOGICIELS ET DES APPLICATIONS

Identification du partenaire responsable et description des modalités de gestion des différentes versions de ces actifs essentiels.

4. DÉCRIRE PRÉCISEMENT LES DIFFÉRENTES GESTIONS ATTACHÉES AUX SAUVEGARDES PAR TYPE DE RESSOURCE

Serveur(s) – Ressource(s)

Responsable(s) – Intervenant(s)

Périodicité des sauvegardes – Jours - Horaires

Suivi et contrôle des sauvegardes (journaux, fichiers résultats, destinataires,...)

Description de la solution mise en œuvre

Pour une solution interne

- Type de support
- Identification des supports (type de données – sensibilité – date ...)
- Modalités de rangement et de récupération
- Suivi et contrôle des sauvegardes (journaux, fichiers résultats, destinataires ...)
- Description des modalités de transfert périodique de sauvegardes sur un site distant (mode d'externalisation, mesures de protection, conditionnement, contrôle à l'envoi / à la réception, récupération ...)
- Modalités des tests de relecture et de restauration (fréquence, intervenants, publication des résultats ...)
- Identification des personnels habilités aux différentes gestions

Pour une solution externe, le contrat doit prévoir toutes les dispositions indispensables à la préservation des intérêts de l'entreprise

- Engagement en responsabilité et en confidentialité du fournisseur
- Plan de sauvegarde, plan d'assurance sécurité du fournisseur
- Protection des données sensibles
- Droit d'audit
- Réversibilité de la solution
- Propriété des informations
- Traçabilité des opérations ...

Nous l'avons évoqué, un tableau récapitulatif des principales informations pour chaque type de sauvegarde peut trouver sa place en annexe du plan.

Il ne peut remplacer la rédaction des informations détaillées indispensables à la garantie des gestions pour l'ensemble des intervenants.

LES COMMENTAIRES APPORTEES PAR LES LECTEURS DE L'ARTICLE

Cette annexe propose un complément d'informations à partir des commentaires reçus pour cet article. C'est un apport précieux à l'amélioration de son contenu. Nous remercions vivement leurs auteurs.

- **LE CHIFFREMENT**, la politique de Sécurité de l'Information doit s'en préoccuper, le plan de sauvegarde doit le mentionner pour chaque ressource concernée, afin de considérer les dispositions spécifiques à prendre dans le cadre de la préservation et de la restauration de ces données²
- **LE RISQUE DE PERTE DE DONNEES LORS DU NETTOYAGE DE BASES**, notamment à l'échéance de périodes de rétention d'informations, sauf à ... prévoir ce type d'opération au plan de sauvegarde
- **LES PRECAUTIONS A PRENDRE LORS D'UN CHANGEMENT DE SYSTEME DE SAUVEGARDE**, c'est-à-dire ... prévoir l'intégration de tests de rechargement des données dans le cadre de cette opération délicate.

² Indispensable à la protection de données et de transactions de sensibilité majeure, le chiffrement est à pratiquer avec ... tact et mesure.

Gestion des clés et des annuaires, accès aux données chiffrées, utilisation ... Il est, en effet, porteur de risques opérationnels qu'il convient de prendre en compte dans l'analyse de besoins, dans la définition de la solution, dans sa mise en œuvre et son suivi