Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

n° 972-1/SGDN/DCSSI

Paris, le 17 juillet 2003

GUIDE TECHNIQUE

pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter

(Problématique de « l'effacement » des signaux magnétiques)

Mots clés : signaux magnétiques, confidentialité, support magnétique, disque dur, surcharge, effaceur, effacement, démagnétiseur, démagnétisation, destruction.

DIRECTION CENTRALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Version : 1.12/2004

SOMMAIRE

1 : REFERENCES

[1] **Directive n°515/SGDN/SSD/DR du 03/06/83 sur la protection du secret de défense en bureautique,** voir :
Annexe 1 : Tableau risques/parades des matériels de bureautique, à la ligne : *Stockage*, la parade n° 6 : « Effacement contrôlé du support (destruction si effacement impossible) ».

[2] **Recommandation n°600/DISSI/SCSSI, édition de mars 1993, sur la protection des informations sensibles ne relevant pas du secret de défense,** voir :
4.3 Destruction des résidus
4.3.2 : « Les supports magnétiques amovibles (…) doivent être effacés (…) ».
5.4 Fichiers
5.4.5 : « Destruction : les fichiers sensibles périmés doivent être effacés (…) ».
5.6 Dépannage
5.6.1 : « (…) effacement des mémoires, (…), des informations sensibles, (…) ».

[3] **Recommandation n°901/DISSI/SCSSI du 02/03/94, pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.**

[4] **Directive n°911/DISSI/SCSSI/DR du 20/06/95, relative aux articles aux articles contrôlés de la sécurité des systèmes d'information,** voir :
Paragraphe 20.5, alinéa c) : Méthodes techniques d'effacement des mémoires

[5] **Guide pratique pour la protection des supports classifiés de défense n°972/SCSSI/SI du 09/04/98**, voir :
Chapitre 8. Effacement d'un support pour recyclage interne.

[6] **Schéma de qualification des solutions de surcharge de sécurité des disques durs, n°972-3/SGDN/DCSSI, document provisoire du 17/07/03.**

2 : AVANT PROPOS

Les mesures du guide [5] s'appliquent pour la protection des supports classifiés de défense. La plupart de ces mesures peuvent s'appliquer pour la protection des supports contenant des informations sensibles non classifiées de défense. Mais leur application aux supports magnétiques ne permet pas de bénéficier pleinement du caractère réutilisable de ceux-ci. Quand de tels supports sont soumis à des exigences de gestion et de sécurité qui s'opposent, il convient de mener une analyse de risque pour les informations qu'ils contiennent et de la confronter à une évaluation des charges induites par les mesures de sécurité identifiées. A l'issue, il sera possible de déterminer les mesures justes à appliquer.

3 : OBJET DU GUIDE

Ce guide a pour objet la confidentialité des informations enregistrées sur les supports magnétiques quand survient le besoin de recycler ou exporter ces supports.

Il s'applique pour la protection des informations enregistrées sur les supports magnétiques classifiés de défense[1] et pour la protection des informations sensibles non classifiées de défense enregistrées sur des supports magnétiques.

Il est à l'usage des responsables de l'organisation de la sécurité des systèmes d'information de l'administration. Il s'adresse aussi aux responsables budget-finances et aux gestionnaires des parcs informatiques de l'administration.

Les supports magnétiques considérés dans ce guide sont les « disques durs ».

4 : DEFINITIONS

Les définitions suivantes fixent la terminologie du guide :

Support réutilisable[2] **:** média qui permet l'écriture de telle façon que les données précédemment écrites peuvent devenir inaccessibles dans les conditions normales d'exploitation du média.

Support magnétique[3] **:** média sur lequel des données sont écrites et lues grâce à des champs magnétiques ; un support magnétique est réutilisable par nature.

Disque dur : système constitué d'un ou plusieurs supports magnétiques, appelés **plateaux**, et d'un sous système, appelé **têtes**, composé d'éléments mécaniques, électroniques et logiques, qui effectue les transcriptions, l'écriture et la lecture des données.

Ecriture : opération qui place des signaux magnétiques rémanents sur les plateaux.

Lecture : opération qui mesure les signaux magnétiques rémanents sur les plateaux.

[1] Il complète le guide [5].
[2] Cette définition corrige celle du guide [5], paragraphe : 6.2.2.
[3] Cette définition actualise celle du guide [5], paragraphe 6.1.1.

Effacement : opération qui supprime les signaux magnétiques rémanents sur les plateaux.

Accès logique : méthode d'acquisition de données au moyen des têtes du disque dur contrôlées soit par la logique implantée dans ces têtes[4], soit par une autre logique.

Accès physique : méthode d'acquisition de données avec des moyens d'investigation sensibles aux traces perceptibles directement sur les plateaux.

Recyclage : changement dans l'emploi d'un disque dur sans changer d'environnement de sécurité[5].

Exportation : envoi d'un disque dur hors de son environnement de sécurité[5].

5 : PROBLEMATIQUE

Les disques durs possèdent deux fonctions qui permettent, en condition normale d'exploitation, deux opérations : l'écriture et la lecture. L'effacement n'est pas possible, sauf à concevoir et implanter dans les disques durs une fonction nouvelle[6] ou définir avec les deux fonctions existantes un processus dont les effets seraient jugés équivalents à ceux de l'effacement.

Un disque dur qui implanterait un mécanisme de démagnétisation des plateaux disposerait d'une fonction d'effacement. Si la capacité de cette fonction à supprimer les signaux magnétiques rémanents sur les plateaux était reconnue[7], le disque dur qui l'implanterait, serait qualifié : **disque dur démagnétisable** (ou **effaçable**) **de sécurité**.

Un processus qui ajouterait des signaux magnétiques rémanents sur les plateaux d'un disque dur par dessus les signaux magnétiques rémanents anciens rendrait ces derniers difficiles à mesurer. Si la capacité de ce processus à empêcher la mesure des signaux magnétiques rémanents anciens était reconnue[8], le processus produirait l'effet de sécurité attendu de l'effacement. Il serait qualifié : **surcharge de sécurité**.

6 : ANALYSE DE RISQUE

Le **besoin de sécurité** pris en compte est la confidentialité des informations écrites sur les disques durs destinés à être recyclés ou exportés.

L'**objectif de sécurité** retenu pour satisfaire ce besoin est l'inaccessibilité des informations écrites sur les disques durs avant leur recyclage ou leur exportation.

[4] C'est la **condition normale d'exploitation** d'un disque dur.
[5] Un **environnement de sécurité** est un système d'information soumis à une politique de sécurité (PSSI).
[6] Telle que celle des lecteurs-enregistreurs de bandes magnétiques qui implantent, en plus des têtes d'écriture et de lecture, une tête de démagnétisation dite aussi « tête d'effacement ».
[7] Conformément à un schéma de qualification validé par la DCSSI.
[8] Conformément au schéma de qualification [6].

L'identification et le choix des mesures pour atteindre cet objectif s'appuie sur la distinction des menaces et l'évaluation des risques correspondants.

Les menaces font l'objet d'une typologie qui distingue cinq niveaux de capacité hostile :

[M1] Accès logique aux données en se servant de privilèges « utilisateur » et des commandes du système d'exploitation courant.

[M2] Accès logique aux données en se servant de privilèges « administrateur » et des commandes du système d'exploitation courant, ou d'un système d'exploitation connu.

[M3] Accès logique aux données en se servant d'un système d'exploitation spécial qui utilise des commandes « bas niveau » spécifiques au disque dur[9] attaqué.

[M4] Accès physique aux signaux analogiques par les têtes, et reconstitution des données.

[M5] Accès physique aux traces laissées sur les plateaux, et reconstitution des données.

Les risques sont évalués à partir d'hypothèses sur les probabilités d'attaques, leurs impacts et les vulnérabilités des systèmes d'informations qui recyclent ou exportent des disques durs.

Analyse du risque pour les disques durs soumis aux menaces [M1]-[M2]

Les attaques qui surviennent contre les disques durs recyclés sont le plus souvent non intentionnelles. Il s'agit de demandes d'accès légitimes à des données avec les navigateurs, les moteurs de recherche, les programmes d'exploration, d'administration ou de maintenance. Ces demandes peuvent conduire à la divulgation d'informations dont l'accès aurait dû être empêché. La probabilité des attaques non intentionnelles est élevée. Toutefois l'impact de ces attaques est nul dans les systèmes dont l'homologation de sécurité garantit la bonne gestion des droits d'accès aux informations. En revanche, dans les environnements permissifs[10], cet impact ne devrait pas être négligé ; des informations peuvent être révélées fortuitement. Pour réduire ce risque, **il est recommandé de remédier à la permissivité de l'environnement et d'appliquer, avant le recyclage, des mesures de sécurité élémentaires** (*tableau n° 1*).

Si des comportements déviants d'agents placés dans le circuit du recyclage sont envisagés, il convient de considérer que des supports recyclés seront soumis à des investigations, y compris avec des outils commerciaux, ou libres, de récupération de données. L'impact des attaques devrait être nul dans les systèmes dont l'homologation de sécurité garantit la bonne gestion des droits d'accès aux informations. En revanche, dans les environnements permissifs, l'impact est certain et immédiat ; des informations seront révélées. Pour réduire ce risque dans les systèmes d'information qui font l'objet d'une homologation de sécurité, **il est recommandé de dissuader ou d'empêcher toutes formes de comportement déviant et d'appliquer, avant le recyclage, des mesures de sécurité élémentaires** (*tableau n° 2*). Pour réduire le risque dans les environnements permissifs, **il est recommandé de remédier à la permissivité de l'environnement, de dissuader ou d'empêcher toutes formes de comportement déviant et d'appliquer, avant le recyclage, des mesures de surcharge** (*tableau n° 3*).

[9] Les commandes « bas niveau » spécifiques aux disques durs sont celles que les constructeurs se réservent et ne documentent généralement pas ; elles ne sont pas spécifiées dans les normes ATA.
[10] Environnement sans politique, ni solution efficace, de gestion des droits d'accès au système d'exploitation.

Il convient enfin de considérer que les disques durs exportés seront soumis à des investigations systématiques avec les moyens courants et des moyens connus, y compris des outils commerciaux ou libres de récupération de données. L'impact des attaques est certain et immédiat ; des informations seront révélées. Pour réduire ce risque seul, **il est recommandé d'appliquer, avant l'exportation, des mesures de surcharge** (*tableau n° 4*).

Analyse du risque pour les disques durs soumis à la menace [M3]

Cette menace suppose des attaques menées avec des moyens logiques spécialement conçus pour récupérer des données numériques sur un type ou un modèle de disque dur. La mise au point et la mise en oeuvre de tels moyens nécessitent de connaître parfaitement les caractéristiques techniques détaillées des disques durs attaqués. Il est peu probable que de tels moyens soient accessibles aux usagers ordinaires et que leur mise en œuvre dans un environnement de sécurité correctement administré passe inaperçue. Cette menace est considérée improbable dans le cas du recyclage.

En cas d'exportation, il convient de considérer que des supports seront probablement soumis à des investigations conduites avec des outils logiques spécialisés. Cette probabilité croît avec le potentiel attractif des informations enregistrées sur les supports et, de façon indépendante, avec les succès qui valident les attaques et l'ampleur de la diffusion du modèle attaqué. Leur impact est certain. Il peut être rapide. Des informations seront révélées. Pour réduire ce risque, **il est recommandé de n'exporter que les disques durs démagnétisables de sécurité qualifiés après activation de leur fonction de démagnétisation** (*tableau n° 4*).

Analyse du risque pour les disques durs soumis aux menaces [M4]-[M5]

Ces menaces supposent des attaques menées avec des moyens importants pour la récupération physique des signaux analogiques ou des traces sensibles et leur transcription vers un système de données exploitables. Elles ne concernent pas les disques durs recyclés.

En cas d'exportation, il convient de considérer que des supports seront probablement sélectionnés[11] pour être soumis à des investigations menées avec des moyens importants. Cette probabilité croît avec le potentiel attractif des informations enregistrées sur les supports. Elle décroît avec les difficultés rencontrées pour récupérer les signaux ou les traces sur les plateaux et avec la complexité des calculs à mener pour reconstituer l'information. L'impact des attaques physiques est aléatoire. Il ne peut être immédiat. En cas de succès, des informations seront révélées. Pour réduire ce risque, **il est recommandé de n'exporter que les disques durs démagnétisables de sécurité qualifiés après activation de leur fonction de démagnétisation** (prise en compte de la menace M[4]) **ou de renoncer à l'exportation** (prise en compte de la menace M[5]) (*tableau n° 4*).

[11] Exemple : des supports portant des marques de protection ou provenant d'organismes objets d'attentions intelligentes particulières.

Les quatre tableaux suivants indiquent l'évolution du risque en fonction des mesures de sécurité adoptées, pour chaque menace prise en compte et pour chaque situation considérée dans l'analyse de risque.

Nota : la notation ε représente la mesure d'un niveau de risque réduit.

Tableau n°1. Situation : recyclage, pas de comportement déviant, système permissif.

Mesures / Menaces	aucune	élémentaires(*)	surcharge	effacement(**)	destruction
[M1]		ε			0
[M2]		ε			0

(*) Ces mesures doivent être accompagnées de mesures de réduction de la permissivité de l'environnement.
(**) Cette mesure est applicable aux seuls disques durs démagnétisables de sécurité qualifiés.

Tableau n°2. Situation : recyclage, prise en compte des comportements déviants, système homologué.

Mesures / Menaces	aucune	élémentaires(*)	surcharge	effacement(**)	destruction
[M1]		ε			0
[M2]		ε			0

(*) Ces mesures doivent être accompagnées de mesures de dissuasion, ou d'empêchement, des comportements déviants.
(**) Cette mesure est applicable aux seuls disques durs démagnétisables de sécurité qualifiés.

Tableau n°3. Situation : recyclage, prise en compte des comportements déviants, système permissif.

Mesures / Menaces	aucune	élémentaires	surcharge(*)	effacement(**)	destruction
[M1]			ε		0
[M2]			ε		0

(*) Cette mesure doit être accompagnée de mesures de réduction de la permissivité de l'environnement et de dissuasion, ou d'empêchement, des comportements déviants.
(**) Cette mesure est applicable aux seuls disques durs démagnétisables de sécurité qualifiés.

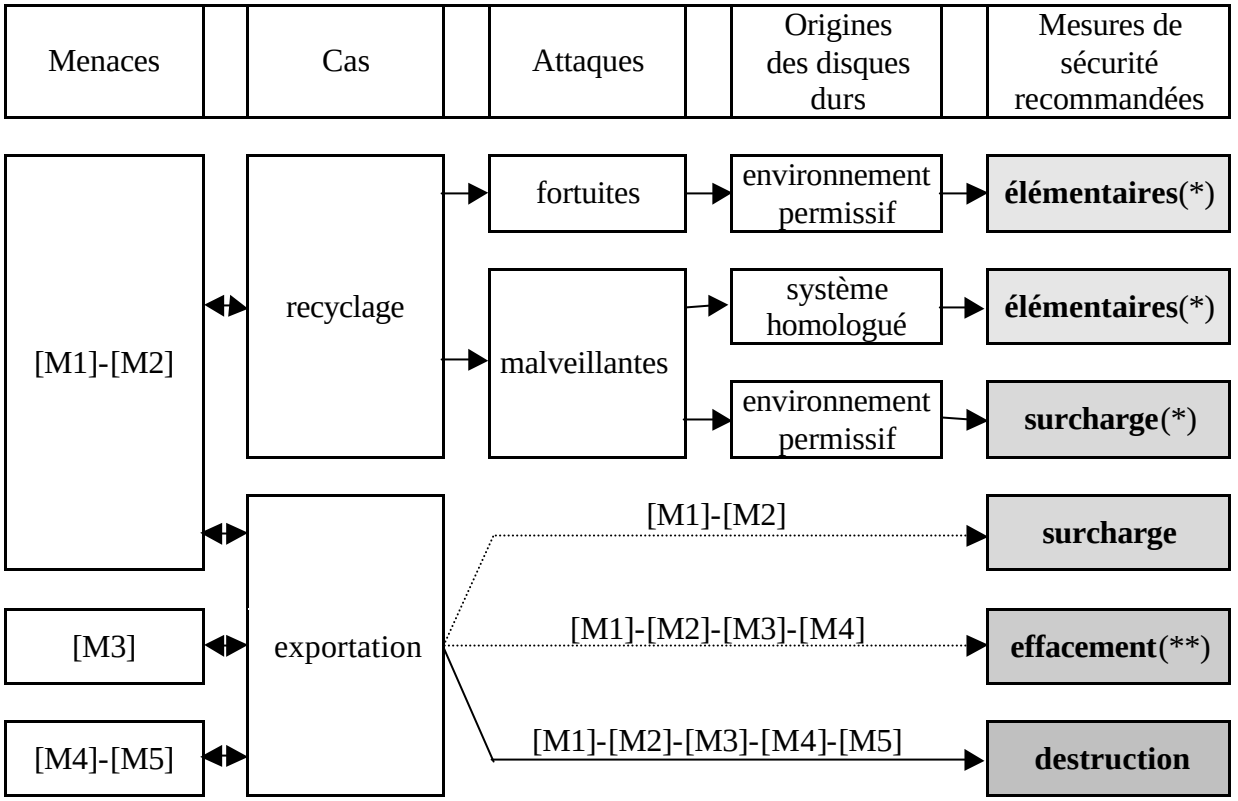
Tableau n°4. Situation : tout cas d'exportation.

Mesures / Menaces	aucune	élémentaires	surcharge	effacement(*)	destruction
[M1]	ε				0
[M2]	ε				0
[M3]			ε		0
[M4]			ε		0
[M5]					0

(*) Cette mesure est applicable aux seuls disques durs démagnétisables de sécurité qualifiés.

Le tableau suivant est un arbre de décisions simplifié qui récapitule les situations analysées.

Tableau récapitulatif de l'analyse de risque.



(*) Ces mesures doivent être accompagnées de mesures de réduction de la permissivité de l'environnement et de dissuasion, ou d'empêchement, des comportements déviants.

(**) Cette mesure est applicable aux seuls disques durs démagnétisables de sécurité qualifiés.

⋯▶ Indique la mesure de sécurité recommandée pour faire face aux seules menaces inscrites sur la flèche.

7 : MESURES DE SECURITE

L'analyse de risque a indiqué quatre catégories de mesures de sécurité :

1- mesures élémentaires,
2- mesures de surcharge,
3- mesures de démagnétisation[12],
4- mesures de destruction.

A noter que la destruction atteint complètement et de façon indiscutable l'objectif de sécurité.

Quand des exigences de gestion et de sécurité s'opposent, il convient de confronter l'analyse de risque à l'évaluation des charges induites par les mesures de sécurité identifiées. L'estimation de ces charges est du ressort des gestionnaires de parcs informatiques et des responsables de l'organisation de la sécurité des systèmes d'information. Ils peuvent préciser pour leurs propres cas l'analyse macroscopique présentée ci après.

Tout d'abord, la charge de la mesure de destruction doit être établie. Elle sert de référence. Si une mesure de sécurité présente des charges moindres tout en se rapprochant suffisamment de l'objectif de sécurité, elle pourra lui être préférée. Dans le cas inverse, l'opportunité de la destruction sera démontrée.

Le calcul de la charge de référence doit prendre en compte la charge de l'opération de destruction des disques durs telle que décrite dans le guide [5] (*Chapitre 9 et Annexe C.6.2*), à laquelle il convient d'ajouter la charge de remplacement[13] des disques durs détruits et leur réinstallation[14].

Pour les catégories de mesures n°1, 2 et 3, les charges s'évaluent à partir de la connaissance des processus opératoires qui leur correspondent, des moyens à mettre en œuvre et des compétences qu'il est nécessaire de mobiliser.

1- Charges générales des mesures élémentaires

Cas du recyclage des disques durs

La mesure élémentaire de sécurité concernant les disques durs à recycler comme articles de maintenance est le formatage complet[15] de toutes leurs partitions avec l'utilitaire de formatage du système d'exploitation courant. Le déroulement du processus est à surveiller. En cas d'interruption, le disque dur est vérifié. Le processus est repris ou le disque dur est déclaré en panne.

[12] Cette mesure est applicable aux seuls disques durs démagnétisables (ou effaçables) de sécurité qualifiés.
[13] La charge de remplacement des disques durs détruits doit se limiter au coût net de remplacement. Les considérations sur la complexité des acquisitions de matériels informatiques sont hors propos. Les gestionnaires de parcs informatiques maîtrisent le renouvellement de leurs équipements pour peu que les ressources soient mises en place en cohérence avec les exigences de la politique de sécurité.
[14] La réinstallation d'une configuration logicielle opérationnelle doit être prise en compte. En effet, le recyclage ou l'exportation à des fins de réemploi, d'un ordinateur sans système d'exploitation, ni applications sous licence est un non sens. Par ailleurs, il faut que la comparaison des charges avec les mesures élémentaires soit possible.
[15] Certains systèmes d'exploitation offrent l'alternative formatage rapide ou complet.

Mise en garde n°1 : la suppression des partitions n'est pas toujours une bonne pratique car elle est susceptible de créer une partition principale d'une taille telle que certains systèmes d'exploitation courant ne pourront pas formater la totalité du disque dur.

Cas du recyclage des ordinateurs

Les mesures élémentaires de sécurité sont des bonnes pratiques pour l'installation d'un poste de travail. Deux processus opératoires font partie de ces bonnes pratiques.

Processus A :
Isoler l'ordinateur ; réinstaller complètement le système d'exploitation en optant pour le formatage complet de toutes les partitions des unités physiques et logiques ; réinstaller les applications utiles ; dé-fragmenter les partitions, s'il y a lieu ; régler et vérifier le bon fonctionnement de l'ordinateur et de ses applications.

Charges :
- ✓ Récupération de tous les supports d'installation (système d'exploitation, applications, correctifs, mises à jour et pilotes) avec leur documentation, les clefs et numéros de licence.
- ✓ Récupération des caractéristiques de l'ordinateur, de ses composants et des périphériques qui lui restent associés.
- ✓ Conduite du processus et traitement des interruptions.
  - Le processus peut prendre plusieurs heures par ordinateur.
  - Le processus mobilise un informaticien système.

Processus B :
Isoler l'ordinateur ; installer l'image originale[16] du disque dur en suivant les prescriptions de l'éditeur de l'application de gestion d'images validées par un informaticien système ; si une partition n'est pas concernée par le processus, elle est formatée complètement ; dé-fragmenter les partitions, s'il y a lieu ; régler et vérifier le bon fonctionnement de l'ordinateur et de ses applications.

Charges préparatoires :
- ✓ Recherche, acquisition et prise en main d'une application de création, de maintenance et d'installation d'images de disques durs.
- ✓ Mise au point d'une configuration originale de l'ordinateur valable si possible pour une catégorie d'ordinateurs ; création et sauvegarde de l'image de cette configuration.
- ✓ Mise à jour de l'image au rythme de l'évolution ou de la maintenance de la configuration ; à défaut, la charge de mise à jour sera reportée après l'étape d'installation de l'image et s'ajoutera aux charges opératoires.

Charges opératoires :
- ✓ Conduite du processus et traitement des interruptions.
  - Le processus prend quelques minutes par ordinateur[17].
- ✓ Installation des correctifs, mises à jours des pilotes qui ne seraient pas dans l'image.
  - Le processus mobilise un informaticien système.

[16] A condition de disposer de cette image (appelée aussi : clone ou master) ; voir les charges masquées.
[17] Dans le cas où toutes les charges masquées sont assumées par ailleurs.

Mise en garde n°2 : le processus B ne doit pas être réduit à la seule opération de formatage des partitions de données s'il y en a; cette opération laisserait intactes les données qui ont transité normalement par les autres partitions.

2- Charges générales des mesures de surcharge

Les mesures de surcharge de sécurité visent à placer sur toute la surface de tous les plateaux des disques durs, des signaux magnétiques nouveaux sensés masquer les signaux magnétiques rémanents anciens. Elles mettent en œuvre des solutions logicielles qualifiées conformément au schéma [6]. Ce schéma est à la disposition des responsables de l'organisation de la sécurité des systèmes d'information de l'administration.

Processus opératoire :
Isoler l'ordinateur ; démarrer à partir du support de la solution (disquette, CD-ROM) ; valider les avis émis par la solution ou renoncer à poursuivre ; choisir la stratégie de traitement ; valider le rapport de fin des opérations.

Charges préparatoires :
- ✓ Conception ou recherche d'une solution de surcharge.
- ✓ Qualification de la solution de surcharge disponible.
- ✓ Acquisition et prise en main de la solution de surcharge de sécurité retenue.
- ✓ Mise en place d'une alimentation stabilisée pour l'ordinateur isolé.

Charges opératoires :
- ✓ Raffinement de l'analyse de risque et choix de la stratégie de surcharge.
- ✓ Conduite de l'opération de surcharge et traitement des interruptions.
  - Le processus prend quelques dizaines de minutes à plusieurs dizaines d'heures par ordinateur, en fonction de la stratégie de surcharge, de la taille du disque dur et des performances de l'ordinateur.
- ✓ Validation du rapport de fin des opérations.
- ✓ Réinstallation des disques durs traités[18] (*voir les charges des processus A et B*).
  - Le processus mobilise un informaticien système.

Charge induite :
- ✓ Vieillissement prématuré des disques durs traités.

3- Charges générales des mesures de démagnétisation

Les mesures de démagnétisation ne s'appliquent qu'aux disques durs démagnétisables (ou effaçables) qualifiées conformément au schéma de qualification qui leur est spécifique.

Processus opératoire :
Isoler l'ordinateur ; lancer l'effacement en suivant les prescriptions du constructeur du disque dur validées par un informaticien système.

[18] Uniquement dans le cas du recyclage ou de l'exportation d'ordinateurs complets ; il est nécessaire de comptabiliser cette charge pour pouvoir comparer les charges des quatre catégories de mesure.

Charges préparatoires :
- ✓ Recherche de disques durs démagnétisables (ou effaçables).
- ✓ Qualification des disques durs démagnétisables (ou effaçables) trouvés.
- ✓ Surcoût d'acquisition des disques durs démagnétisables (ou effaçables) qualifiés.

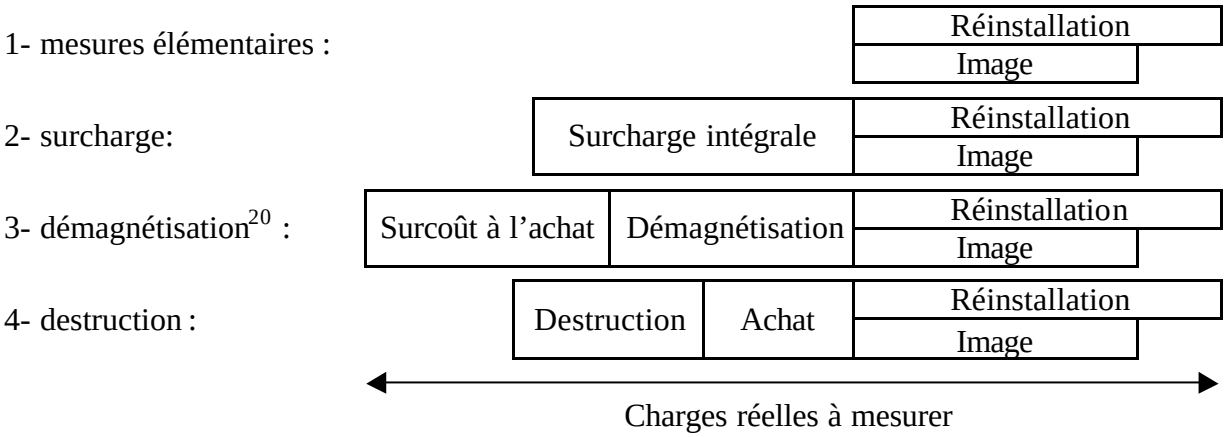
Charges opératoires :
- ✓ Conduite de l'opération de démagnétisation et traitement des interruptions.
- ✓ Réinstallation des disques durs traités[19] (*voir les charges des processus A et B*).
  - La durée d'une telle opération n'est pas connue.
  - Les compétences nécessaires pour conduire un telle opération ne sont pas connues.

Mise en garde n°3 : un ordinateur en panne ne permet généralement pas d'appliquer de mesures de sécurité à son disque dur ; pourtant sa mise en réparation correspond la plupart du temps à une exportation qui soumet le disque dur aux menaces [M3] et plus ; en cas de mise en réparation hors de l'environnement de sécurité, il convient d'établir les règles suivantes :

Règle n°1 : un disque dur en état de fonctionner, ou jugé tel, n'accompagne pas un ordinateur mis en réparation.

Règle n°2 : un disque dur en panne, ou jugé tel, se voit appliquer les mesures de destruction.

Tableau de comparaison des charges.



8 : CONCLUSION

A l'issue de l'analyse de risque et de l'évaluation des charges induites par les mesures de sécurité, la liberté de choisir la mesure juste dépend de l'existence de solutions.

Ce guide a identifié les catégories de mesures qui répondent le mieux au problème posé. Il ne présume pas de l'existence de solutions qualifiées pour chaque catégorie. Seuls des projets et des appels d'offres sont susceptibles de faire évoluer la qualité et la quantité des solutions.

La satisfaction de certaines exigences demande encore de l'invention, sauf à reconnaître l'entreprise absurde au regard des économie réalisables et des risques encourus.

[19] Uniquement dans le cas de l'exportation d'ordinateurs complets ; il est nécessaire de comptabiliser cette charge pour pouvoir comparer les charges des quatre catégories de mesure.

[20] Cette mesure est applicable aux seuls disques durs démagnétisables de sécurité qualifiés.