Guide de bonnes pratiques organisationnelles pour les Administrateurs Systèmes et Réseaux

dans les unités de recherche

..

Olivier Brand-Foissac

Laurette Chardon

Marie David

Maurice Libes

Gilles Requilé

Alain Rivet

Contact : gbp@listes.resinfo.org

Table des matières

INTRODUCTION

Définitions - Objectifs

Le terme "guide" est défini comme suit dans plusieurs dictionnaires : "*qui donne des conseils et accompagne*". En ce qui concerne les « bonnes pratiques », la définition de Wikipédia semble convenir au guide que nous élaborons :

*"Le terme « **bonnes pratiques** » désigne, dans un milieu professionnel donné, un ensemble de comportements qui font consensus et qui sont considérés comme indispensables, qu'on peut trouver sous forme de guides de bonnes pratiques (GBP). Ces guides sont conçus par les filières ou par les autorités. Ils peuvent se limiter aux obligations légales, ou les dépasser. Comme les chartes, ils ne sont généralement pas opposables. Ils sont souvent **établis dans le cadre d'une démarche qualité** par les filières."*

Comme cela été les cas pour les deux précédentes productions de RESINFO : SiLabo [SiLabo] et EcoInfo.[EcoInfo], ce projet de guide est né de plusieurs réflexions liées aux différents contextes de travail de notre métier dont on peut citer celui, largement partagé, de l'augmentation et de l'intensification des tâches d'exploitation des systèmes informatiques et réseaux ainsi que des responsabilités attenantes, et ce, la plupart du temps, à moyens humains constants.

Son objectif est donc de proposer aux Administrateurs Systèmes et Réseaux (ASR) nouveaux entrants, ou déjà en place, de mieux identifier les processus essentiels nécessaires pour fournir le service aux utilisateurs, sécuriser nos serveurs et réseaux, documenter nos actions, communiquer, gérer notre temps, respecter certaines contraintes juridiques, se former, etc

Il permettra sans doute d'aider à la structuration du travail dans nos activités, voire à améliorer l'organisation des services informatiques des unités de recherche et en définitive la qualité de service.

Bien sur nous intégrons dans les "Bonnes Pratiques" de l'ASR la prise en compte des conséquences sur l'environnement de l'utilisation de l'informatique. Mais il n'y aura pas de chapitre consacré à ces aspects car le groupe de travail ECOINFO de RESINFO a déjà réalisé un gros travail sur ce thème et présente sur son site (http://www.ecoinfo.cnrs.fr) des recommandations concernant entre autres "les problématiques de la consommation énergétique et de la pollution liées à l'utilisation et au développement de l'outil informatique".

Ce guide n'est pas un livre de solutions techniques toutes faites, de "recettes" ou de "trucs et astuces". Les « FAQ » et les « HOWTO » comblent déjà ces besoins techniques depuis longtemps. Il n'est pas non plus un document administratif qui va dicter aux ASR une méthode d'organisation ou leur apprendre à travailler.

Il s'agit plus modestement de s'initier, d'une manière pragmatique, à des méthodologies d'organisation issues à la fois du monde industriel et des normes en matière de fourniture de service et de gestion de la sécurité, mais aussi de synthèses de jurisprudences visant à observer un comportement conforme aux règlements, ou encore d'ouvrages sur la gestion du temps, et enfin de pratiques de terrain déjà mises en œuvre par les ASR de la communauté éducation-recherche.

Nous avons recensé un ensemble de tâches souvent récurrentes et invariantes dans le métier d'ASR et les avons encadrées par un ensemble de "bonnes pratiques" souvent issues des normes qui permettent d'organiser le travail. Cette organisation contribuant in fine à améliorer la qualité du service.

Un cadre minimal proche du terrain

S'adressant à l'ensemble de la profession, une des difficultés qui a du être prise en compte est que cette pratique quotidienne est très variée, à la fois à cause des contextes forts différents d'exercice du métier, mais aussi par la diversité des tutelles des laboratoires et des missions confiées aux collègues (références aux fiches métiers et emploi types). Chacun ne sera donc pas concerné par l'ensemble des sujets abordés dans ce guide mais y trouvera des repères "gradués" qu'il pourra adapter à sa situation. Cependant, en dépit de ces différences de contexte, nous essayerons, quand cela est possible, de définir un cadre minimal pour identifier des tâches de base incontournables à prendre en charge.

Les aspects de mise en œuvre pratique d'organisation de service et de démarche qualité, extraits de ITIL et ISO-20000 que nous décrivons dans ce guide peuvent parfois paraître difficilement repérables ou directement applicables par les ASR. En effet ces notions d'organisation et de qualité de service sont jusqu'à présent peu intégrées à nos habitudes de travail dans nos unités de recherche.

Pour ne pas rester trop théorique, nous donnons en fin du guide un ensemble de *références techniques* vers des logiciels ou de la bibliographie qui peuvent permettre aux ASR de mettre en place tel ou tel processus nécessité dans l'organisation de service. L'ASR reste de toute façon maître bien sûr de ses choix techniques dans son propre contexte.

Bonnes pratiques et Qualité

Le terme "qualité" est utilisé ici en référence aux projets de "Démarche Qualité en Recherche" qui se développent dans nos laboratoires mais qui ne prenaient pas en compte jusqu'à présent la spécificité du métier d'ASR. A titre de rappel, il sera précisé plus largement dans le chapitre ce que l'on entend par "démarche qualité".

Le terme "Guide des Bonnes Pratiques" a été choisi en référence au "Guide de Bonne Pratique de Laboratoire" (BPL) élaboré en 1998 par l'OCDE en vue d'assurer, initialement, la qualité et la validité des données d'essai servant à établir la sûreté des produits chimiques.

Les recommandations initiées ont été prolongées et formalisées dans une politique de "Démarche Qualité" propre au contexte de la recherche scientifique s'appuyant en particulier sur des normes internationales (européennes et françaises comme ISO-9001 et maintenant ISO-20000). Ces normes permettent d'assurer des références communes et d'apporter des "garanties" de qualité dans les relations entre divers partenaires dans le cadre de collaborations internationales (scientifiques ou industrielles) via des certifications et des agréments délivrés par des organismes habilités.

Le projet du Groupe de travail de RESINFO à l'origine de ce guide peut donc s'inscrire dans le cadre général d'une "Démarche Qualité" avec comme idée directrice de contribuer à rendre plus « lisibles » les missions, l'organisation de nos services et finalement notre travail vis à vis de nos directions et tutelles et nous aider à son amélioration continue.

Pour autant ce Guide des Bonnes Pratiques n'a pas pour objectif d'être un modèle pour préparer une accréditation ou un agrément.

Si la référence (indispensable) aux quelques normes et standards en vigueur utilisés dans le monde industriel (ITIL ou ISO-20000), pouvant concerner directement notre métier, est présente (et elle sera explicitée) c'est essentiellement pour se conformer à l'existant et fixer des repères identifiables dans la classification de ce qui est exposé.

Dans ce cadre nous utiliserons aussi le concept de "processus" proposé par les documents normatifs pour décrire l'organisation efficace de la fourniture de service .

Nous retiendrons donc comme définition d'un « processus » celle définie par la norme ISO-9001 de Système de Management de la Qualité comme « un ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en élément de sortie » [ISO-9001].

Il convient donc d'identifier et de gérer les diverses activités (et processus) en interaction dans l'exercice quotidien de notre métier. Cette structuration pourra alors, si besoin, servir de base pour un projet local de démarche qualité intégré dans la politique du laboratoire.

Les contraintes relevant des tutelles

La démarche utilisée a aussi tenu compte des "contraintes" contextuelles et obligations relevant des tutelles auxquelles sont soumis les ASR dans l'exécution de leurs tâches. Parmi celles-ci la politique de sécurité concernant les systèmes d'information en fonction de leur contexte en est un bon exemple. Elle sera bien sûr abordée (elle fait aussi l'objet d'une normalisation sous le label ISO-27001 et est déclinée au CNRS sous le nom de PSSI [PSSI CNRS]). Il ne s'agira pas de se substituer aux structures compétentes pour dicter des lignes de conduite mais plutôt d'indiquer les points qui sont susceptibles d'impacter la pratique des ASR.

Les contraintes juridiques

Nous tentons de dégager quelles sont les bonnes pratiques dans le contexte des responsabilités juridiques ? En effet, le travail des ASR est désormais en prise avec de nombreuses obligations et responsabilités de nature juridique. Dans le cadre de la protection du Système d'Information (S.I), la responsabilité administrative et pénale de la hiérarchie et des ASR peut être recherchée. Il conviendra donc de connaître les principaux règlements en matière de cyber protection (LCEN, informatique et liberté) relatifs à la protection de la propriété intellectuelle, des données relevant de la vie privée (fichier nominatifs), et les comportements professionnels qu'ils induisent.

Les bonnes pratiques liées aux contextes personnel et relationnel des ASR

Un autre point essentiel et rarement abordé dans les formations initiales ou continues est la gestion du temps. Fortement soumis aux sollicitations quotidiennes des utilisateurs, l'ASR doit aussi mener en parallèle des tâches de "fond" qui nécessitent une continuité d'attention et de travail. Ces aspects seront eux aussi spécifiquement abordés pour donner quelques pistes de gestion du temps dans ce domaine à partir de méthodes relevées dans des ouvrages réalisés à ce sujet et transposées à notre métier.

On traitera enfin des aspects du métier qui requièrent de la méthode mais aussi des capacités d'organisation personnelle (gestion du temps, agenda, planning..), des qualités de communication, de compréhension et souvent de diplomatie vis à vis de nos utilisateurs. On examinera dans quel contexte d'organisation et d'interface avec les collègues du laboratoire, ces techniques sont mises en œuvre. Une partie sera réservée à la mise à niveau des compétences. Les compétences sont fortement évolutives dans notre métier et nécessitent de s'intéresser à la veille technologique et à la formation professionnelle : comment l'ASR peut (et doit) s'adapter et évoluer dans un métier sujet à des avancées technologiques importantes.

Enfin, parallèlement à ces avancées technologiques, dans le cas de regroupement de laboratoires ou de l'organisation de services à l'échelle des campus par exemple, des tendances à la mutualisation se font jour ; une bonne organisation du travail et une lisibilité des solutions mises en œuvre est un gage de bonnes collaborations à différents niveaux de la structure. En ce sens ce guide peut fournir une base commune d'identification des processus métiers.

Bonne lecture

Remerciements :

Nous remercions la MRCT (« Missions des Ressources et Compétences Technologiques ») du CNRS [http://www.mrct.cnrs.fr] pour son support logistique, ainsi que F. Berthoud, B. Perrot, E. Drezet, MN Branlé, D. Baba, et JM Barbet qui ont bien voulu consacrer un peu de leur temps pour relire ce guide et nous faire part de leurs avis et corrections.

LES BONNES PRATIQUES DANS LA FOURNITURE DE SERVICES INFORMATIQUES

1- Une démarche qualité dans les unités de recherche

1.1- Description des modèles ITIL et ISO-20000

Les recommandations sur l'organisation des services informatiques qui vont être exposées ci-après sont issues d'une réflexion fortement inspirée de l'approche de l'amélioration de la qualité des services des S.I. (Systèmes d'Information) décrite par ITIL [ITIL] (Information Technology Infrastructure Library) et plus récemment par la norme ISO-20000.[ISO-20000].

La norme ISO-20000, prolongement du référentiel ITIL, fournit un modèle pour la gestion de services informatiques. Cette norme formalise l'ensemble des activités d'une production informatique et correspond à une approche « orientée client » qui introduit la notion de « qualité de service » apportée aux utilisateurs. Dans le cadre de l'activité informatique, on peut définir le service comme un échange à valeur ajoutée matérialisé par un flux.

Aujourd'hui, les organisations métiers ont des attentes fortes sur la qualité des services fournis par l'informatique et ces attentes évoluent. Dès lors, le service informatique doit se concentrer sur la qualité de service, en d'autres termes, rendre les services correspondants aux besoins aux coûts appropriés.

Il nous a semblé opportun de nous référer à ITIL et ISO-20000 qui fournissent un cadre dans lequel positionner les activités et méthodes existantes des services informatiques tout en favorisant leur structuration. Ainsi, parmi les processus métiers présents dans la norme ISO-20000, on distingue ceux relatifs à la fourniture de service et ceux relatifs au support de service.

La « fourniture de services » décrit les processus nécessaires pour fournir le service aux utilisateurs et comporte les processus suivants :

- la gestion des niveaux de service
- la gestion de la continuité et la disponibilité
- la gestion de la capacité
- la budgétisation
- la gestion de la sécurité

Le « support de service » décrit les processus nécessaires pour mettre en place et assurer un service efficace et fonctionnel. Il est composé des processus suivants :

- la gestion des configurations
- la gestion des changements
- la gestion de la mise en production
- la gestion des incidents
- la gestion des problèmes

A ces processus « métier », s'ajoutent les processus de la boucle PDCA (voir définition paragraphe suivant) destinés à formaliser l'ensemble des activités qui concernent l'amélioration continue avec en autres :

- les rôles et responsabilités de la Direction,

- la gestion documentaire,
- la gestion des compétences et de la formation,
- la surveillance et la mesure

La méthode PDCA (Plan Do Check Act), encore appelée roue de Deming [Deming], comporte 4 étapes qui consistent successivement à planifier des actions en réponse à des objectifs (Plan), les mettre en œuvre (Do), puis contrôler l'efficacité des solutions par rapport aux objectifs au moyen d'indicateurs (Check). Avec la quatrième étape (Act), on va chercher à corriger et améliorer le système mis en place ce qui conduit à élaborer un nouveau projet et initier un nouveau cycle.

Entreprendre une démarche de « bonnes pratiques » c'est en effet mettre du bon sens et développer ses capacités d'initiative au service de l'amélioration de la qualité en apprenant à identifier, faire, mesurer et analyser de façon progressive afin de travailler plus efficacement et, à terme, gagner du temps.

1.2- Transposition au contexte ASR dans une unité de recherche

En replaçant ce modèle d'organisation dans le contexte d'une unité de recherche, les auteurs ont posé comme préalable que les processus décrits doivent être identifiables et mesurables dans l'ensemble des services informatiques de nos entités CNRS, Universitaires, EPST ou EPIC... sur la base d'un « plus petit dénominateur commun ». Les bases d'organisation ainsi posées ne doivent pas être restrictives et doivent pouvoir se décliner en fonction du contexte et du périmètre des unités de recherches (taille, mono ou multi site, diversité des recherches, collaborations internationales…). Ainsi, l'application de cette démarche qualité au métier d'ASR dans un laboratoire de recherche et sa spécificité nous conduisent à proposer un modèle d'organisation décrit plus précisément au cours des chapitres suivants.

1.2.1- Définir le périmètre d'action

Comme préalable à toute organisation, l'ASR doit, dans un premier temps, définir son périmètre d'action en spécifiant ses domaines d'intervention et/ou en excluant les domaines qui ne sont pas de sa responsabilité, ceci pouvant fortement conditionner la nature de ses activités.

1.2.2- Mettre en place une gestion des configurations

Ce processus s'intéresse à la gestion de l'infrastructure informatique. Cette étape nécessite d'effectuer un inventaire de l'ensemble des composants aussi bien matériels (ordinateurs, équipements réseau …) qu'immatériels (documentations, licences, contrats…) du service.

1.2.3- Définir les niveaux de service

La définition des niveaux de service doit permettre aux utilisateurs de connaître la nature et l'étendue du support offert par le service informatique. Chaque « niveau de service » sera associé à des objectifs réalistes visant à assurer un niveau de qualité satisfaisant à la fourniture de ce service.

1.2.4- Définir la continuité de service

Associé à chaque niveau de service, l'ASR devra spécifier les exigences des utilisateurs de l'unité en termes de continuité des services. Cet engagement établi en accord avec la Direction (et/ou une commission d'utilisateurs) sera évalué régulièrement.

1.2.5- Gérer les interventions

Il convient de prendre en compte de manière efficace toutes les demandes d'intervention qu'il s'agisse de demandes d'intervention des utilisateurs ou de changements à apporter aux éléments du système.

1.2.6- Gérer les dysfonctionnements

L'objectif consiste, d'une part, à minimiser l'impact des dysfonctionnements du système d'information sur les services et d'autre part, à prévenir leur réapparition.

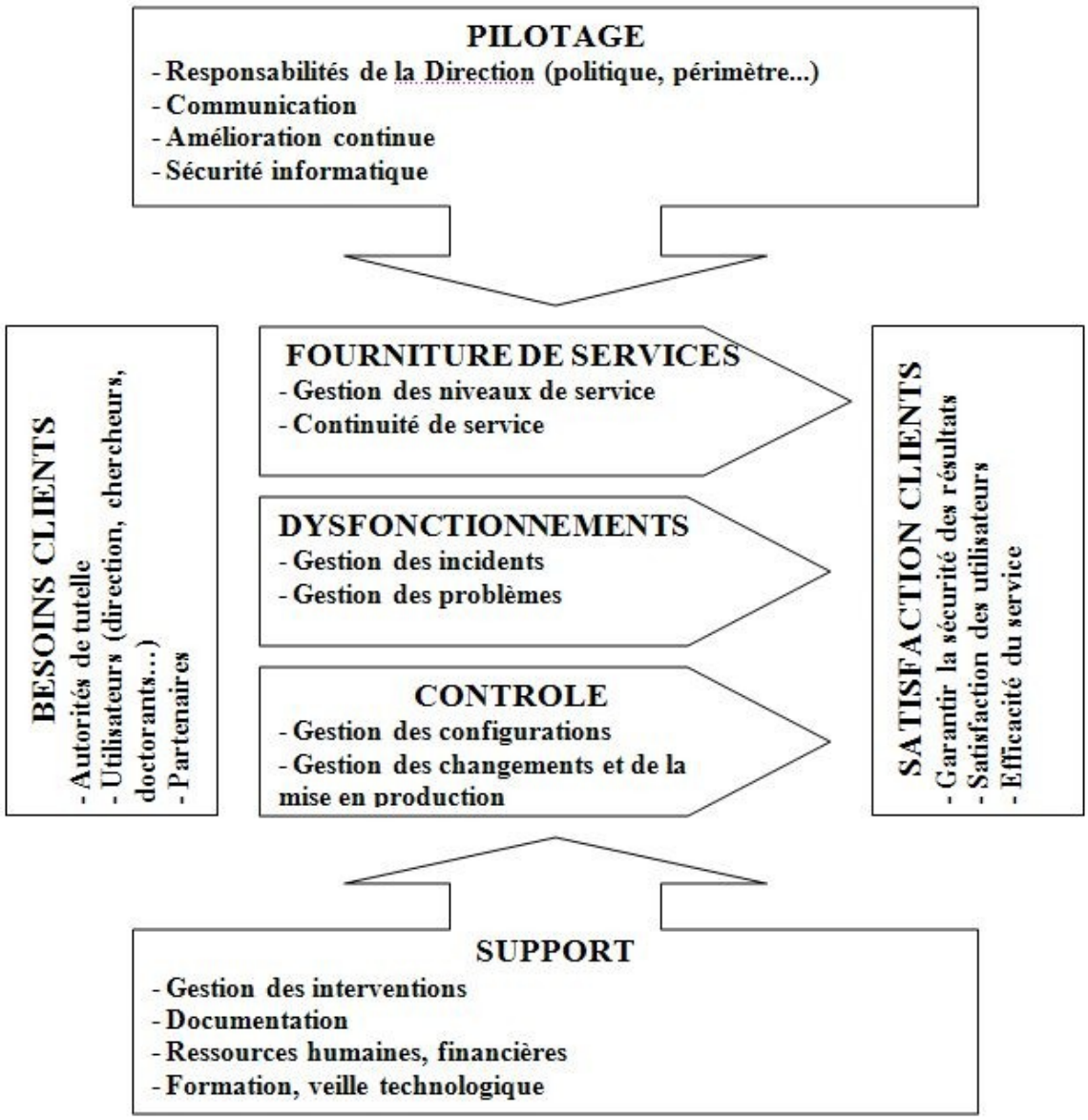
1.2.7- Assurer les changements et mise en production

Tout changement apporté au système d'information doit être maîtrisé afin de minimiser le risque d'incident potentiel lors de sa mise en place.

La gestion de la sécurité s'appuie sur un référentiel à lui tout seul, l'ISO-27001 [ISO-27001] qui sert de base à la mise en place des politiques de sécurité au sein des unités. Elle sera développée dans un chapitre particulier de ce guide.

A travers ce guide, nous essayerons de préciser d'une part, ce qui nous parait comme essentiel à mettre en place au sein d'un service système d'information et d'autre part, ce vers quoi il convient de tendre, ces deux niveaux pouvant être considérés comme deux niveaux de maturité de l'organisation du système d'information d'une entité de recherche.

Adaptés à nos structures d'entités CNRS, Universitaires, EPST, EPIC, etc., les concepts ITIL/ISO-20000 peuvent être visualisés au travers de la cartographie suivante :



Cartographie des processus dans un laboratoire de recherche

Les processus de pilotage et de support complètent dans cette cartographie les processus métier représentés par la fourniture de services, la gestion des dysfonctionnements et le contrôle. La norme introduit la notion de « client » : autorités de tutelle, utilisateurs du service (la direction, les chercheurs…) ou partenaires que l'on va chercher à satisfaire. Cette satisfaction va, par exemple, consister à garantir la sécurité des résultats de la recherche, répondre aux besoins des utilisateurs tout en améliorant l'efficacité du service.

1.3- Définition du périmètre

La fonction première d'un service informatique d'une unité de recherche est de « participer à la réalisation des objectifs métiers de l'unité ». Pour réaliser ces objectifs, le service informatique doit mettre en œuvre un certain nombre de processus au travers d'un certain nombre de services fournis dans un périmètre donné. Une des questions les plus délicates qui se pose au préalable est la définition du périmètre sur lequel vont porter les processus énoncés précédemment.

Nous avons précisé que l'objectif des recommandations de bonnes pratiques sur le plan organisationnel était de tendre vers un plus petit dénominateur commun aux services informatiques des unités de recherche. Il en va de même pour le périmètre à considérer.

Dans le cadre de la mise en place des processus d'organisation, il faut se garder de vouloir envisager « tout et tout de suite ». Pour être plus précis, il est nécessaire de respecter des paliers progressifs de maturité dans l'élaboration de ces bonnes pratiques et dans la définition du périmètre et de rester pragmatique en fonction des ressources humaines disponibles et de la taille de l'unité. A cet effet, il faut se poser les questions suivantes :

- quels sont les métiers de l'unité que le service informatique soutient ?
- quels sont les besoins exprimés par les utilisateurs de l'entité : les « clients »?
- quels sont les champs d'activités définis et validés : quel est par exemple le périmètre de l'administration réseau au sein du laboratoire ? Le DNS, le serveur de messagerie, le réseau sans fil… sont-ils pris en charge directement par le laboratoire ou par une autre structure de type CRI ?
- quels sont les éléments matériels et logiciels que le service informatique gère dans le périmètre précédemment défini ?
- et surtout, quels sont les éléments du périmètre à considérer dans un objectif de disponibilité de l'activité « vitale » du laboratoire ?

Dans sa définition minimale, le périmètre d'activité précédemment défini doit intégrer les éléments nécessaires à la continuité de service de l'unité. Par exemple, les serveurs (supports des données de recherche) font partie de ce périmètre ainsi que tous les éléments nécessaires à la continuité de la recherche. On pourra aussi y inclure le matériel actif, les routeurs et commutateurs (s'ils sont gérés par l'ASR), les sauvegardes, la messagerie... Ce périmètre pourra être élargi dans un deuxième temps, lorsque l'organisation de premier niveau sera fonctionnelle.

Il faut bien comprendre que cette phase de définition du périmètre est essentielle. Elle nécessite sans doute une concertation préalable et une prospection de l'existant avec les instances du laboratoire (direction, commission informatique…). La réponse ne sera pas déclinée à l'identique dans toutes les entités, et chaque laboratoire est un cas particulier avec une taille, des moyens et surtout des objectifs différents. Ceci sous-entend une définition claire des missions du service (si la structure existe) et de celles de l'ASR au sein de l'entité de recherche.

2- La gestion des configurations

2.1- Ce qu'il faut prendre en compte

Une fois le périmètre envisagé et de façon à définir les services à fournir, il faut s'appuyer sur un ensemble d'éléments d'infrastructures sur lesquels l'ASR peut/doit agir. Ces éléments d'infrastructure doivent être identifiés et classés dans une base de connaissances qui sera tenue à jour régulièrement.

Dans la terminologie ITIL/ISO-20000, l'ensemble de ces informations constitue la base des configurations connue sous le terme de CMDB (Configuration Management DataBase). Cette base doit être maintenue et mise à jour régulièrement en fonction des modifications intervenues sur les différents éléments d'infrastructure.

La gestion des configurations est une des conditions nécessaire et préalable à la gestion de l'ensemble des autres processus. Elle permet de suivre avec efficacité l'évolution des infrastructures informatiques, et d'en assurer la gestion et l'exploitation.

Les éléments de configuration sont les biens matériels ou immatériels qui composent les services offerts dans le périmètre qui a été défini. Par exemple on peut y trouver : les serveurs, postes de travail, imprimantes, autres périphériques, logiciels, licences, équipements réseaux, comptes informatiques, consommables, documentations techniques, contrats...

Pour bien identifier les composants devant figurer dans la base de gestion des configurations, on s'attachera à répondre aux questions suivantes :

- quels composants matériels utilisons-nous aujourd'hui ?
- quels équipements doivent être remplacés ?
- quels contrats de maintenance avons-nous et doivent ils être revus ?
- quelles licences avons-nous et sont-elles en règle ?
- à quels réseaux un équipement est il connecté ?
- quels sont les composants utilisés et par qui ?
- quels composants sont impactés par un déploiement, lesquels sont responsables d'une erreur ?
- comment l'équipe des ASR du laboratoire partage ses connaissances ?
- quelle documentation est mise à disposition des utilisateurs et comment ?

La gestion des configurations se doit de fournir aux autres processus des informations précises et pertinentes sur les composants du système d'information. Ces informations permettent d'identifier rapidement le composant touché par un incident. Elles permettent aussi, par exemple, de calculer les coûts de la maintenance et des licences logicielles.

Dans sa définition minimale, la base de connaissances des configurations doit comprendre tous les éléments d'infrastructure compris dans le périmètre minimal défini précédemment**.**

Dans une réflexion plus élargie, les objectifs de la gestion des configurations sont les suivants :

- rendre compte de tous les biens et configurations de la production informatique de l'unité.

- fournir de l'information pertinente sur les configurations pour supporter les autres processus (gestion des niveaux de service : qu'est-ce que l'on doit maintenir, comment ? gestion des changements : qu'est-ce qui doit être changé, quelles incidences sur les autres éléments ?...).
- fournir des bases solides pour la gestion des dysfonctionnements.
- comparer l'information stockée à l'infrastructure en place et corriger les différences.

2.2- Comment organiser la gestion des configurations

Il faut se garder de vouloir détailler trop précisément les éléments d'infrastructure afin de conserver la maîtrise de l'ensemble sans perte de temps (ne pas faire « d'usine à gaz »). Il est par ailleurs important d'avoir un contrôle efficace sur les configurations si l'on veut maîtriser correctement ce processus. Ainsi, toute modification apportée par un utilisateur à la configuration de son matériel doit pouvoir être identifiée et répertoriée.

Pour cela il convient de définir le niveau de granularité, c'est-à-dire le niveau de détail des éléments de configuration que l'on veut appliquer (équilibre entre détail et facilité de gestion). Le principe général pour définir le bon niveau est d'avoir le maximum de contrôle sur les éléments avec un minimum de travail d'enregistrement, en intégrant principalement les éléments qui ont un réel impact sur les niveaux de service. Par exemple doit-on considérer un ordinateur (poste de travail ou serveur) comme élément de configuration ou doit-on rentrer dans le détail en prenant en compte ses composants (cartes réseau et graphiques, disque dur, graveur...).

Le niveau de détail est défini en terme « *d'attributs* » des éléments de configuration dont voici quelques exemples à considérer (au sein de la *CMDB)* :

- catégorie (matériel, logiciel, document…)
- numéro de série (matériel, logiciel)
- numéro de version (logiciel, documentation)
- numéro de licence (logiciel)
- numéro d'inventaire du matériel
- fournisseur
- emplacement (site, local)
- date achat, date de mise à jour, date de fin de garantie….
- responsable, utilisateur…
- composant principal ou sous composant de (relations entre les composants)
- statut ou cycle de vie (opérationnel, en cours de changement,...)
- historique des interventions, ...

La gestion des configurations peut être opérée de façon simple, à partir d'un outil tableur par exemple ou de manière plus sophistiquée et automatique avec des outils de gestion de parc.

On trouvera dans la partie Fiches de références techniques de ce guide un certain nombre de pointeurs vers des logiciels ou de la documentation qui peuvent servir et être utilisés par les ASR pour implémenter et mettre en place les différents volets requis dans la qualité de service.

3- La gestion des niveaux de service

3.1- Déterminer les services à considérer

La gestion des niveaux de service doit permettre :

- de déterminer le niveau de service à délivrer aux utilisateurs pour supporter les métiers de l'unité de recherche,
- d'initialiser un suivi pour identifier si les niveaux demandés ont été atteints et dans le cas contraire, pourquoi.

Le but de la « Gestion des Niveaux de Service » est de définir, de maintenir et d'améliorer progressivement la qualité des services rendus par l'ASR pour assurer les activités de l'unité.

Il convient donc, au cours de ce processus, de définir les niveaux de service fournis par l'ASR en relation avec les besoins des utilisateurs. Nous pouvons citer par exemple quelques niveaux de service couramment supportés par les ASR dans nos entités : *la gestion du parc informatique, la maintenance des serveurs, la surveillance réseau, le déploiement d'application, les sauvegardes, l'archivage, l'assistance de premier niveau aux utilisateurs….*

Les niveaux de service ainsi définis sont référencés dans un catalogue de services. On pourra les hiérarchiser par type de service :

- service métier*: Disponibilité des moyens de calcul, de visualisation graphique, développement informatiques dédiés, support à la gestion financière et RH...*
- service infrastructures *: gestion des serveurs, des sauvegardes, des impressions...*
- services réseaux *: gestion de la disponibilité du réseau...*
- service applicatif *: messagerie, web...*
- etc.

L'ASR qui veut mettre en place une gestion de niveau de service doit s'assurer au préalable , auprès de ses utilisateurs, des services qu'ils utilisent et comment. Ainsi, le cycle de la qualité de service passe par un engagement entre le service informatique et les utilisateurs du laboratoire identifiés dans des structures métier (la direction, les services administratifs, les équipes de recherche).

Pour estimer le niveau de service minimal, il faut se rapprocher du périmètre envisagé, des infrastructures gérées et du seuil critique pour la continuité de l'activité.

Dans un deuxième temps, on peut envisager, de graduer en trois catégories principales les niveaux de service à apporter :

- vital : un service dont l'interruption bloque complètement le travail dans le laboratoire. *Exemple : le service d'annuaire LDAP si l'authentification de connexion sur les machines passe par une authentification LDAP, les routeurs/commutateurs et le contrôleur de domaine si une grande majorité des PC sont sous Windows et nécessite une authentification.*
- important : un service qui peut être interrompu brièvement. *Exemple : messagerie, web, sauvegarde, serveurs calcul, serveur anti-virus.*
- normal : un service qui peut être interrompu quelques jours .*Exemple: un PC, une imprimante, un serveur de licence logicielle.*

3.2- Quel niveau pour quel service ?

La formulation d'un niveau de service dans le catalogue des services peut comporter :

- la description du service offert,
- les fonctions métiers couvertes,
- les périodes de fonctionnement du service,
- la disponibilité du support,
- le plan de secours,
- le plan de reprise…

Deux paramètres sont à considérer pour définir le degré de service à proposer :

- l'existence de besoins différents par groupe d'utilisateur : par exemple le niveau de service pour les secrétariats d'administration et de scolarité, ne seront sans doute pas les même que ceux pour un groupe de chercheurs *(gérer les sorties d'imprimante pour le service scolarité en période d'inscription semble plus vital que pour un groupe de chercheurs en période moins drastique)*
- l'existence de contraintes différentes liées aux types d'infrastructures.

Plusieurs questions posées au préalable peuvent aider l'ASR à déterminer les niveaux de service :

- A-t-on mesuré et validé la qualité de service de l'application avant sa mise en production ?
- Nos utilisateurs reçoivent-ils un service conforme à nos engagements ?
- Peut-on mesurer la qualité de service en temps réel ?
- Dispose-t-on d'un système d'alerte efficace pour gérer les incidents d'exploitation en temps réel ?
- Dispose-t-on d'un historique du niveau de service ?
- Peut-on identifier un problème avant qu'il ne réduise la qualité de service ?
- A-t-on une visibilité et un contrôle suffisants du fonctionnement de nos applications métier critiques ? …

4- La gestion de la continuité de service

L'objectif de la gestion de la « continuité de service » (en corollaire à la gestion des niveaux de service) est de diminuer durablement la fréquence et la durée des incidents en s'assurant que l'infrastructure informatique et la fourniture de service qui est associée peuvent être remises en route dans les temps requis et convenus.

Depuis plusieurs années, l'interdépendance entre activités métiers et activités informatiques est parvenue à un point tel que si les services informatiques offerts s'arrêtent, une grande part des activités de recherche peut être fortement impactée. L'activité de recherche nécessite de plus en plus un fonctionnement 7/7 et 24/24 du système d'information et des services informatique.

La gestion de la continuité de service consiste à :

- identifier, par une méthode d'analyse de risques, les menaces et les vulnérabilités sur les actifs de l'infrastructure,
- appliquer dans un deuxième temps des mesures (préventives et de reprises) qui permettent de conserver un niveau de continuité de service.

La gestion de la continuité de service doit donc s'accompagner d'un plan de continuité de service (actions d'urgences, sauvegardes des enregistrements vitaux, évaluation des dommages, plan de reprise...)

Le contenu de ce plan pourra prendre en compte :

- la/les procédures de déclenchement de ce plan,
- les équipements couverts par le plan,
- la description des procédures de continuité définies,
- les responsabilités et impacts sur les ressources humaines,
- les impacts sur la sécurité (en mode dégradé),
- les procédures de retour à la normale,
- les procédures de test du plan de continuité…

5- La gestion des interventions

5.1- Ce qu'il faut prendre en compte

L'objectif principal de la gestion des interventions est de simplifier et formaliser la chaîne de demande d'assistance en provenance de l'utilisateur tout en augmentant la réactivité du service. Cette fonction nécessite de prendre en compte l'ensemble de l'intervention, de l'appel de l'utilisateur, jusqu'au retour de sa demande après résolution du problème.

Il s'avère également essentiel pour un ASR de mémoriser les demandes de façon à pouvoir recenser l'ensemble des interventions effectuées au niveau du S.I. Les informations ainsi recueillies permettront, d'une part, d'assurer un meilleur suivi des interventions et, d'autre part, de disposer d'un historique des demandes et de statistiques.

Tout utilisateur étant amené à effectuer une demande d'intervention, l'objectif de la gestion des interventions va consister à fluidifier leur traitement. A cet effet, l'ASR devra mettre en place un circuit de décision : filtrer les demandes, en déterminer la priorité et les catégoriser, le choix de la priorité devant intégrer une analyse de risque et s'effectuer en concertation avec l'utilisateur.

A ce stade, l'ASR doit se demander quel niveau d'intervention il doit prendre en charge et quel type d'intervention va nécessiter un suivi précis.

5.2- Comment organiser la gestion des interventions

Ce premier niveau de la gestion des interventions qui s'avère essentiel pourra être réalisé différemment selon les méthodes de travail des ASR (cahier de laboratoire, fichier numérique, outils logiciels de type « helpdesk »…).

A un deuxième niveau de maturité du système, la gestion des interventions pourra se complexifier. Deux points seront alors à prendre en considération.

5.2.1- Optimiser les ressources pour accélérer le traitement des interventions

Dans le cas d'un nombre important d'interventions ponctuelles, la saisie d'un appel doit être rapide et sûre de façon à récupérer l'ensemble des données de l'utilisateur et les motifs de son appel, ces informations pouvant faire l'objet d'une fiche d'appel très structurée (coordonnées, descriptif, date, intervenant…). Au retour d'intervention, la fiche permettra son suivi : temps passé, solution adoptée, fourniture …

L'affectation des ressources, quelles soient matérielles ou humaines, s'effectuera à partir de cette fiche et une planification de l'intervention sera mise en place.

5.2.2- Analyser les interventions

Des tableaux d'analyses découleront des interventions effectuées. Cette synthèse pourra prendre plusieurs formes :

- tableaux de bord,
- recherches multicritères sur les interventions,
- base de connaissances,

- rapports statistiques à personnaliser (ex : nombre d'interventions par mois ...)

Cette analyse des interventions pourra constituer, par ailleurs, un paramètre de mesure de l'activité du service. Son évaluation régulière permettra de suivre l'amélioration de son fonctionnement dans le cadre du modèle PDCA inhérent à la norme ISO-20000.

6- La gestion des dysfonctionnements

L'objectif essentiel de ce processus est de chercher à résoudre les dysfonctionnements susceptibles de se produire au sein d'un S.I. Il s'agit de minimiser leurs répercussions sur les niveaux de service mais également de prévenir leur réapparition. Les référentiels ITIL et ISO-20000 décrivent la gestion des dysfonctionnements en deux processus distincts, la gestion des incidents et la gestion des problèmes.

La norme ISO-20000 distingue la notion d'incident de celle de problème. Un incident est « tout événement qui ne fait pas partie des opérations standards d'un service, et qui provoque ou peut provoquer une interruption de service ou altérer sa qualité » alors qu'un problème est considéré comme la « cause inconnue et sous-jacente d'un ou de plusieurs incidents ».

6.1- La gestion des incidents

La gestion des incidents va consister à rétablir les services le plus rapidement possible. Tout incident devra être enregistré et documenté de façon à tracer les opérations qui ont été nécessaires à sa résolution.

Outre la description originelle de l'incident, l'enregistrement devra être mis à jour tout au long du cycle de vie de l'incident, de façon à pouvoir par la suite communiquer sur celui-ci.

L'enregistrement pourra ainsi comporter les informations suivantes :

- la catégorie (réseau, station, service, organisation...),
- la date,
- la priorité,
- les services impactés,
- le statut (nouveau, en cours, résolu...)

6.2- La gestion des problèmes

La gestion des problèmes vise à rechercher la cause première des incidents récurrents et nécessite de mettre en place un suivi d'actions pour améliorer ou corriger la situation. C'est pourquoi, de façon à traiter correctement et rapidement un incident récurrent qui se présente, il est indispensable que les informations sur les incidents soient disponibles.

La gestion des problèmes va comprendre deux types d'actions :

- les actions correctives : il s'agit, dans un premier temps, d'identifier les causes des incidents passés et résoudre les problèmes en réponse à ces incidents et, dans un deuxième temps, de formuler des propositions d'amélioration et de correction.
- les actions préventives : il s'agit de l'identification et de la résolution des problèmes connus avant que les incidents ne surviennent. On cherche donc à prévenir l'apparition des problèmes en identifiant les faiblesses du S.I. et en proposant des solutions pour les éliminer. Cela va consister à définir des axes d'amélioration qu'il conviendrait d'apporter au système. En alimentant ainsi le système d'amélioration continue, cette gestion pourra servir à la justification de demandes de nouvelles acquisitions ou remplacement de matériels nécessaires au bon fonctionnement du service (virtualisation des services...)

Par la suite, l'ASR pourra affiner la gestion des dysfonctionnements à partir des questions suivantes :

- comment différencier les responsabilités entre la gestion des incidents et la gestion des problèmes ?
- comment communiquer auprès des utilisateurs sur les incidents ?
- comment gérer dans certaines situations le « conflit d'intérêt » qui peut exister entre la résolution d'un incident et la résolution du problème associé (le redémarrage immédiat d'un serveur peut conduire à l'effacement de certains fichiers logs qui auraient être utiles à la résolution du problème) ?
- comment formaliser les solutions mises en place ?

Là encore, toute latitude est laissée à l'ASR pour définir les méthodes et outils qu'il convient d'utiliser pour mettre en place cette gestion des dysfonctionnements.

7- La gestion des changements et de la mise en production

Les changements au sein d'un service S.I. peuvent être multiples et concerner par exemple l'ajout ou la suppression d'un élément de configuration, l'évolution de la version d'un composant voire un changement organisationnel. L'objectif de la gestion des changements et de la mise en production est de réduire au minimum les conséquences des incidents éventuels liés à ces changements sur le système. A cet effet, toute modification, qu'il s'agisse de modifications matérielles (changement de disque, ajout de mémoire …) ou logicielles (mises à jour des systèmes, installation de logiciels…) devra être notifiée de façon à en garder une trace et éventuellement pouvoir revenir en arrière.

Lorsqu'un changement est nécessaire, il faut évaluer les risques de sa mise en œuvre et son impact sur la continuité de l'activité métier pendant et après cette mise en œuvre. Lors de la mise en production, il va s'agir de protéger l'environnement de production et les services associés par l'utilisation de procédures formelles et par des vérifications lors de l'implémentation des changements.

La gestion des changements et de la mise en production consiste à faire évoluer un S.I. de façon structurée sans commettre d'erreurs. On va ainsi chercher à réduire l'impact négatif des changements, améliorer la gestion des dysfonctionnements par une connaissance précise des modifications apportées et donc, à terme, améliorer l'efficacité des services rendus.

Tout changement sera accompagné de tests permettant de valider les modifications apportées. Une solution de repli de type « retour arrière » sera également étudiée. Il est préférable, d'une manière générale, de planifier les changements en fonction de la disponibilité des ressources tout en cherchant à éviter les changements faits dans l'urgence suite à un dysfonctionnement du système.

L'ASR devra donc se poser la question des méthodes et des démarches qu'il convient de mettre en place pour traiter efficacement et rapidement ces changements tels que :

- mettre en place un dispositif adapté à la taille du service,
- mettre en place un planning prévisionnel des changements,
- planifier, par exemple, la mise à jour système des serveurs du laboratoire,
- avertir et informer les utilisateurs de l'interruption de service inhérente au changement de configuration...

Avec un niveau de maturité supplémentaire, l'ASR cherchera à apporter une vue complète du processus et à s'assurer que tous les aspects de ces changements ont bien été pris en compte (tests complets, solution de retour arrière…). A ce niveau, il conviendra de se poser les questions suivantes :

- comment intégrer de façon optimale les processus de gestion des changements et de la mise en production avec la gestion des configurations ?
- comment communiquer sur les changements apportés à l'infrastructure ?

Par ailleurs, un bilan sera mis en place à partir des points suivants :

- l'implémentation s'est-elle bien passée ?
- dans le cas d'une réponse négative, la solution de retour arrière a t-elle pu être réalisée ?

- la planification en termes de ressources était-elle suffisante ?
- l'utilisateur est-il satisfait ?
- y a-t'il eu un effet de bord non prévu ?

8- La Documentation

Nous avons souligné précédemment l'importance de la formalisation des méthodes de travail au sein d'un S.I pour améliorer la qualité dans la fourniture de service informatique. Dans ce cadre, la documentation occupe une place très importante dans le suivi et la traçabilité de nos différentes actions telles que la mise en place de nouveaux services, la gestion des configurations, les changements apportés au S.I., la résolution des incidents et problèmes, l'aide aux utilisateurs, etc.

La réalisation d'une documentation et sa mise à disposition auprès du personnel et/ou des collègues ASR chargés d'intervenir sur les installations apparaissent donc comme des activités support importantes au sein de notre cartographie du S.I. Il s'agit d'une bonne pratique permettant de retrouver l'information voulue au moment voulu, d'assurer la traçabilité des différentes interventions que nous sommes amenés à faire de manière à pouvoir fournir si nécessaire des explications détaillées à la Direction, aux autorités compétentes sur la structure des installations et des services.

Un dépôt documentaire centralisé, riche et bien organisé fera gagner du temps aux ASR. Ces dépôts peuvent être placés par exemple sur un site Web accessible et aisément modifiable par un système de gestion de contenu (CMS comme Drupal ou Spip), ou encore un « Wiki »[wiki].

Dans l'ensemble des tâches qui jalonnent le métier d'ASR, il est donc nécessaire de réserver du temps pour rédiger les diverses documentations nécessaires à la maintenance et à l'évolution du S.I.

On distinguera deux grandes classes de documentation qu'on peut organiser dans deux dépôts distincts : celui destiné aux utilisateurs doit être accessible dans l'intranet de l'unité, alors que le second devrait être réservé aux ASR de par les informations confidentielles qu'il peut contenir.

8.1- La documentation pour les utilisateurs

Ce sont les documents qui permettent aux utilisateurs de comprendre les règles et procédures à suivre pour accéder et utiliser correctement les services qui sont mis en place par le service informatique. Ce type de documentation est très important dans le fait qu'elle peut rendre les utilisateurs autonomes et permet de ne pas faire appel aux ASR et les déranger inutilement pour des questions basiques et récurrentes.

A titre d'exemple, ce type de documentation peut être constitué de :

- un livret d'accueil, établi par le service informatique, qui peut être remis aux nouveaux entrants, et qui peut constituer la base d'une description des services offerts aux utilisateurs. Ce livret peut alors pointer vers des documentations plus complètes détaillant l'utilisation de chaque service mis en place par le Service Informatique.
- les documentations d'utilisation de chaque service en production (par exemple comment utiliser le VPN du laboratoire, comment paramétrer le logiciel « thunderbird » pour accéder à la messagerie, comment se connecter au serveur dédié « ssh », comment paramétrer son PC pour accéder au réseau « Eduroam »...).
- les règlements (souvent rassemblés dans le règlement intérieur de l'entité de recherche) concernant l'utilisation des services, la charte d'utilisation des moyens informatiques, ou encore le document cadre relatif à la politique de sécurité de l'organisme considéré,
- les accords sur les modalités et niveaux de service offerts par l'équipe Informatique, les usages tolérés, les règles de conduite, etc.

8.2- La documentation technique destinée aux ASR

Cet ensemble de documents regroupe les informations techniques nécessaires pour que les ASR mettent en place et fassent fonctionner tel ou tel service. Ce sont les textes techniques propres au service informatique de l'unité et qui peuvent contenir des informations sensibles (plans du réseau, ACL de routeurs mises en place, noms et adresses IP de serveurs sensibles, mots de passe, etc). La qualité de ces documentations doit permettre de confier ou déléguer l'exploitation de certains services à d'autres ASR de l'équipe ou chargés transitoirement d'intervenir.

Une procédure d'exploitation ou d'installation bien documentée est en effet plus facile à déléguer à d'autres ASR de l'équipe et peut faciliter l'intégration d'un stagiaire qui a alors à sa disposition un "mode d'emploi" clair et précis.

Ces documentations doivent donner une image de l'état technique des systèmes (services en exploitation à un temps donné), du réseau, des procédures pour assurer la continuité de service. Ces documentations sont mises à jour régulièrement, lors de chaque modification, pour être au plus près de la réalité.

En effet, comme on l'a vu précédemment dans la « gestion des changements », il est nécessaire pour les ASR d'enregistrer et de documenter les changements apportés dans l'exploitation du système d'information. Il s'agit davantage dans ce cas de constituer et de tenir à jour une « main courante » afin de tracer chronologiquement les changements de configuration apportés dans la configuration de tel ou tel logiciel, ou bien les causes et les résolutions d'incidents qui sont survenus dans le S.I., ou encore l'historique des interventions et des mises à jour.

Comme exemple de ce type de documentation pour les ASR on peut citer :

- le plan à jour du réseau de l'unité, la configuration des commutateurs et des routeurs
- l'inventaire des ressources informatiques
- la documentation des configurations système indiquant comment un service a été paramétré pour l'installer : comment est configuré Samba, comment est assurée la redondance du serveur de mail au moyen de « heartbeat » ou autres systèmes de disponibilité.
- les procédures délicates que l'on fait rarement : par exemple comment reconstruire le « raid » de la baie de disques?
- les procédures d'exploitation récurrentes que l'on veut pouvoir confier à d'autres membres de l'équipe informatique : *comment créer un compte?, comment changer les bandes de sauvegardes?*

Ces informations seront importantes en cas d'incidents ou de dysfonctionnements pour retrouver l'origine possible dans des interventions passées. A cet effet, notons que pour des raisons de disponibilité il serait nécessaire d'assurer une redondance de cette documentation sensible sur support papier de manière à y avoir accès en cas de panne système.

8.3- Comment réaliser ces documentations ?

Le but de ces documentations est qu'elles soient facilement accessibles, modifiables, partageables, correctement structurées, classées et en accès protégé pour les ASR du service uniquement.

L'ASR aura le choix du mode d'édition de ces documentations : documentation papier? fichier au format DocBook [DocBook], site Web ou Wiki [Wiki]?

Les dépôts documentaires de type « wiki » peuvent à cet effet procurer un certain nombre d'avantages :

- leur accès est centralisé sur un serveur Web, ce qui permet de ne pas avoir à chercher la documentation dans de nombreux fichiers et répertoires,
- leur simplicité d'utilisation facilite les mises à jour rapides de la documentation,
- ce type de documentation n'a jamais un caractère définitif. Il convient bien à un système en évolution permanente et on peut l'enrichir facilement à tout moment de dernières remarques ou modifications.

Ces dépôts de type Wiki ont cependant aussi des inconvénients relatifs à la classification des informations et à leur structuration. Il est parfois difficile d'avoir une navigation claire dans un « wiki », et la structuration peut être imparfaite ou mise à mal au fil des mises à jour de la documentation.

Quelle que soit la technologie du support de documentation choisie, il est en tout cas nécessaire de faire attention à assurer une diffusion restreinte des informations que l'on porte dans ce type de documentation du fait qu'elles touchent souvent à la sécurité des installations et de l'infrastructure.

Enfin, n'oublions pas qu'une édition papier de ces documentations est nécessaire en cas de problème systèmes majeur qui empêcherait la consultation.

9- Les bonnes pratiques dans la gestion de la sécurité des systèmes d'information

Les ASR sont confrontés depuis longtemps à des problèmes de sécurité informatique récurrents qui peuvent mettre en péril le fonctionnement du S.I. Ils ont donc régulièrement mis en place des mesures techniques pour protéger les serveurs, le réseau et le parc de PC utilisateurs, et ont donc adapté le niveau de sécurité pour réagir aux nouvelles menaces qui apparaissaient au fil du temps sur le réseau.

La liste des menaces et attaques informatiques est vaste (virus, trojan, scan réseau...) et nous n'en ferons pas l'inventaire ici. Il semble également inutile de proposer une liste exhaustive des solutions techniques de sécurité à mettre en œuvre, tant cela dépend du contexte et du niveau de sécurité recherché.

En revanche, comme nous l'avons fait en première partie avec le standard ITIL et la norme ISO-20000 pour la fourniture de services informatiques, nous avons utilisé la norme ISO-27001 pour donner un cadre aux bonnes pratiques des ASR en matière de gestion de la sécurité dans nos organismes de recherche.

En effet, la sécurité de nos systèmes d'information implique quelques pratiques d'administration et d'organisation de base que l'on retrouve dans la norme ISO-27001, de même que dans les PSSI d'établissement (dont celle du CNRS [PSSI CNRS]).

Ces pratiques sont également basées sur une démarche par « processus » et intègrent le principe d'amélioration continue (PDCA, Roue de Deming) qui vise après avoir mis en place des éléments de sécurité, à surveiller et ré-évaluer leur efficacité.

9.1- Grands principes d'organisation de la sécurité au sein du laboratoire

9.1.1- Définition du périmètre sur lequel doit porter la sécurité du S.I.

Pour déterminer quelles sont les exigences de sécurité de l'information de nos unités, il est nécessaire d'étudier au préalable le contexte, le périmètre de l'entité à sécuriser. Cette étude implique de s'attacher à définir les valeurs propres de l'unité : quelles sont les données et les fonctions essentielles que l'on doit sécuriser pour que l'entité continue à exercer ses missions. Pour chaque donnée et fonction recensée, on s'attachera à déterminer quels sont les besoins de sécurité en termes de « disponibilité », « intégrité » et « confidentialité ».

Les premières étapes sur lesquelles doit se pencher l'ASR est donc :

- d'étudier le contexte de l'entité, rappeler son activité principale, les missions qu'elle doit assurer, les services qu'elle doit rendre et les moyens qu'elle utilise pour parvenir à ses missions... puis,
- de recenser et décrire les différents actifs qui composent le S.I. de l'organisme : faire donc un inventaire des matériels, logiciels, réseau, personnel, locaux... et enfin,
- de recenser et identifier les données et fonctions de l'organisme et savoir sur quels actifs et moyens physiques elles reposent.

9.1.2- Implication de la direction vis-à-vis de la sécurité de l'information

Pour sécuriser convenablement une unité, l'ASR doit s'appuyer sur une politique de sécurité soutenue par sa Direction au moyen de directives claires, d'un engagement démontré, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.

Il est nécessaire que les responsabilités en matière de sécurité de l'information soient définies précisément dans l'entité. La Direction doit demander à son personnel de même qu'aux utilisateurs extérieurs en relation avec l'unité, d'appliquer les règles de sécurité conformément aux politiques et procédures établies par l'organisme.

Une des premières mesures essentielles à prendre est la diffusion d'une « charte de bon usage » des outils informatiques de l'unité. Cette charte est un document interne explicatif des droits et devoirs des utilisateurs en matière d'utilisation des moyens informatiques de l'unité. La charte informatique de l'organisme de tutelle (CNRS, Université ou autre EPST) a pour vocation d'être largement diffusée et mise à disposition pour tout nouvel entrant dans l'unité (par exemple par copie dans le compte des utilisateurs, envoi par messagerie, ou tout autre moyen de diffusion efficace ou officiel).

9.1.3- Coordination de la sécurité de l'information

Les activités relatives à la sécurité de l'information de nos unités de recherche sont en général coordonnées par des personnels ayant des fonctions et des rôles appropriés représentatifs des différentes parties de l'organisme.

Aussi, il convient pour l'ASR d'entretenir ou mettre en place des relations appropriées avec les autorités compétentes et les spécialistes de la SSI de l'organisme, ou encore via des forums spécialisés dans la sécurité et des associations professionnelles.

Que ce soit pour les Universités, le CNRS ou d'autres EPST, il convient pour l'ASR de connaître les acteurs de la chaîne organique et de la chaîne fonctionnelle de sécurité de son organisme : pour le CNRS par exemple les CRSSI (coordinateur régional de la sécurité des systèmes d'information) pour la Délégation régionale, ainsi que le CSSI (chargé de la sécurité du S.I) de l'unité.

9.1.4- Formation et sensibilisation à la sécurité du S.I.

Le personnel doit être régulièrement informé des pratiques de sécurité à suivre (nécessité de mots de passe robustes, attitudes vis a vis des spams, etc), des événements et alertes. Il est important pour l'ASR d'organiser des formations de sensibilisation au sein du laboratoire tant au niveau du personnel en place que des nouveaux entrants et du personnel temporaire. Les formations et messages récurrents d'information que délivrent les ASR permettront de rehausser le niveau de sécurité de l'unité en donnant aux utilisateurs une attitude plus responsable face aux menaces qui pèsent sur le S.I.

9.2- Analyse des données du Système d'Information de l'unité – Analyse des besoins de sécurité

La protection du patrimoine de nos entités suppose d'identifier et de localiser au préalable les données et de déterminer leur niveau de sensibilité. Les besoins en sécurité se définissent en termes

de « confidentialité », de « disponibilité », et d' « intégrité », ainsi que par l'évaluation de leur degré de sensibilité (public, confidentiel, secret défense...). Seul cet examen des besoins peut permettre de déterminer le type de protection nécessaire et les solutions techniques adéquates à mettre en œuvre pour sécuriser le S.I.

La protection de l'outil de travail et du S.I des unités implique la mise en œuvre des moyens techniques pour assurer :

- la disponibilité des moyens informatiques : implique des mesures de redondance, des procédures de reprise sur panne, et un plan de reprise d'activité pour minimiser les temps d'indisponibilité.
- l'intégrité des données : nécessite de mettre en œuvre des procédures de sauvegarde des données, et surtout de restauration de ces sauvegardes.
- la confidentialité des données des utilisateurs : demande d'avoir mis en place des systèmes d'authentification des utilisateurs, ainsi que la mise en place de droits d'accès appropriés sur les données.
- des solutions de « chiffrement »[chiffrement] des supports de données et des protocoles de transmission sont également des outils de nature à assurer une intégrité et confidentialité fortes des données.

9.3- Appréciation des risques

Une analyse des risques (au travers de méthodes telles que EBIOS [EBIOS], MEHARI…), permet d'identifier les objectifs de sécurité et les mesures à prendre, adaptées aux besoins de l'unité. Elle sert de base à l'élaboration de la politique de sécurité du S.I.

Dans un premier temps, il convient d'identifier les menaces et les vulnérabilités potentielles qui pèsent sur les actifs du S.I.

Nous parcourons ici, en quelques phases essentielles, les bonnes pratiques dans le domaine de la sécurisation d'un S.I. La documentation de la méthode EBIOS [EBIOS] peut donner une aide rigoureuse pour sélectionner les menaces et les méthodes d'attaques opportunes dans le contexte étudié.

9.3.1- Identification des menaces et vulnérabilités

Après avoir identifié les « actifs » (matériels, serveurs, routeurs, logiciels, locaux, données...) relevant du périmètre à sécuriser, il convient de recenser les « menaces » qui peuvent peser sur les actifs de l'unité, ainsi que leurs « vulnérabilités ».

Les menaces doivent être formalisées explicitement en identifiant, les méthodes d'attaque auxquelles l'unité est exposée (vol, incendie, perte d'alimentation électrique...), les éléments menaçants qui peuvent les employer (facteurs naturels ou humains, involontaires ou malveillants), les vulnérabilités exploitables sur les entités du système et leur niveau d'occurrence (rare, normal, fréquent).

Par exemple, dans le contexte de l'unité, le vol, l'incendie, l'inondation, la perte d'alimentation électrique, l'incendie, etc peuvent être des éléments menaçants ayant une certaine probabilité d'occurrence (rare, moyenne, certaine...)

On pourra par exemple exprimer une menace de la manière suivante :

- « *l'absence de porte coupe feu dans le couloir peut permettre une propagation plus rapide d'un incendie vers la salle serveur*», ou,
- « *l'accès non contrôlé aux moyens informatiques de la salle serveur peut permettre a un individu mal intentionné d'y pénétrer et de faire d'éventuels méfaits (vols, dégâts..) »*

Seul l'examen de ces menaces et vulnérabilités peut permettre de déterminer les moyens à mettre en œuvre (techniques, procédures, sensibilisation, formation…) pour réduire leur probabilité d'occurrence ou atténuer leur impact.

Enfin, après avoir identifié et formulé les menaces, il est nécessaire de s'attacher à identifier les « *vulnérabilités »* de notre S.I qui pourraient être exploitées par les menaces qui ont été retenues.

Par exemple :

- si le vol est l'élément menaçant qui a été retenu, la salle serveur possède t-elle un système de fermeture adéquat qui permet de réserver l'accès au personnel exploitant ?
- si la perte d'alimentation électrique représente une menace, les serveurs sur lesquels sont stockées les données de l'unité sont-ils correctement secourus électriquement ? Avec une autonomie suffisante ? etc

9.3.2- Identification des impacts

Après avoir identifié les menaces et vulnérabilités du S.I, il faut s'attacher à identifier les impacts qu'ils peuvent induire sur les besoins précédemment exprimés en termes de pertes de confidentialité, d'intégrité et de disponibilité.

Pour chaque menace et vulnérabilité répertoriées, il s'agit d'évaluer la probabilité réaliste d'une défaillance de sécurité ainsi que les impacts associés.

L'ensemble des informations ainsi recueillies va permettre d'estimer les niveaux de risque pour chacun des actifs.

9.4- Traitement des risques

L'étape suivante consiste, à partir de la liste des risques classés par priorité, à définir quels sont les traitements à appliquer pour réduire ou éliminer ces risques :

- retenir et hiérarchiser les risques qui sont véritablement susceptibles de porter atteinte aux fonctions et éléments essentiels de l'entité. Il faut estimer les niveaux des risques, c'est à dire déterminer si les risques sont acceptables en l'état sans mesure de prévention particulière, ou s'ils nécessitent un traitement technique ou procédural particulier.
- définir les objectifs de sécurité permettant de couvrir les risques.

L'ensemble de ces risques devra être évalué, la plupart d'entre eux devant être couvert par des objectifs de sécurité.

Ces objectifs de sécurité constituent le cahier des charges des mesures de sécurité à mettre en œuvre pour l'environnement étudié.

On pourra trouver une liste de mesures de sécurité à prendre dans la norme ISO-27002 [ISO-27002]. Ce document normatif est un « Code de bonne pratique pour la gestion de la sécurité de l'information » et propose toute une série de mesures à mettre en oeuvre pour couvrir les risques révélés par l'analyse.

9.5- Bonnes pratiques dans la mise en œuvre de la sécurité informatique : exemples de mesures de sécurité courante

Voici, ci-après quelques pratiques générales en matière de sécurité informatique qui sont fréquemment mises en place dans la sécurisation du S.I. de nos unités de recherches.

9.5.1- Sécurité physique des locaux

L'objectif est d'empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux dans lesquels résident les informations de l'unité. Les locaux contenant des informations sensibles et des moyens de traitement de l'information (salles serveurs, secrétariat de direction ou d'enseignement...) doivent donc être protégés physiquement des accès incontrôlés ou malveillants (contrôle d'accès par cartes ou code).

Pour se protéger des menaces d'ordre « environnementale », il convient également de mettre en œuvre des dispositifs tels que détection de température élevée, dispositifs anti-incendies, ou inondations, ...

9.5.2- Sécurité du matériel et du câblage

On protégera les matériels sensibles (routeurs, serveurs...) des pertes d'alimentation électrique par un système de secours électrique suffisant, ainsi que d'éventuelles surchauffes par des moyens de climatisation adéquats et bien dimensionnés.

Afin de garantir une disponibilité permanente et un bon fonctionnement en cas de panne, le matériel sensible qui nécessite un fonctionnement continu doit être placé sous contrat de maintenance.

Les accès aux câbles réseau transportant des données doivent être protégés contre toute possibilité d'interception de l'information, ou de dommage. Les câbles ou concentrateurs réseau doivent être hors de portée immédiate et donc protégés dans des gaines ou des armoires de répartition.

9.5.3- Mise au rebut ou recyclage

Les matériels, les informations ou les logiciels ne devraient pas pouvoir être sortis des unités sans autorisation préalable et une procédure formelle. En cas de mise au rebut où de revente de PC, il convient de vérifier que les données ont été effacées des disques de manière efficace. Un simple formatage n'étant bien entendu pas suffisant pour effacer les données de manière pérenne. Des méthodes sont préconisées [A3IMP]

Les supports qui ne servent plus doivent être mis au rebut de façon sûre, en suivant des procédures formelles. Il convient pour des raisons environnementales de même que pour des raisons de sécurité du S.I. de se débarrasser des PC et des supports amovibles dans des bennes spécialisées, après avoir au préalable correctement effacé les supports magnétiques.

9.5.4- Procédures de sécurité informatique liées à l'exploitation :

9.5.4.a- Protection contre les codes malveillants : virus et autres « malwares »

La plupart des attaques via le réseau tentent d'utiliser les failles du système d'exploitation ou des logiciels d'un PC. Les attaques recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parvenir à s'y introduire. C'est pourquoi il est fondamental que les ASR mettent à jour les logiciels des serveurs et des postes clients afin de corriger ces failles.

Suite aux avis de sécurité qui émanent des CERT, l'ASR doit veiller au maintien du niveau de sécurité au cours du temps par l'application récurrente des correctifs logiciels (« patchs ») sur les serveurs en exploitation dans l'unité.

Il est également dans ses fonctions, de veiller à ce que chaque poste du réseau local soit équipé d'un antivirus régulièrement mis à jour. L'ASR doit donc mettre en place des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants.

9.5.4.b- Sauvegarde des informations

La sauvegarde est un processus essentiel dans tout système informatique permettant de garantir l'intégrité des données, la fiabilité et la continuité de l'activité du laboratoire en cas d'incident. Une politique de sauvegarde (fréquence, fenêtre de sauvegarde..) doit être élaborée pour protéger les données de l'unité. Les informations concernant les sauvegardes effectuées doivent être communiquées aux utilisateurs. Une sauvegarde régulière des données des utilisateurs avec des processus de restauration, testée au préalable, doit être mise en place. Il faut porter attention aux droits d'accès à ces sauvegardes.

Des copies de ces sauvegardes doivent être réalisées sur des supports externes (robot de bandes, disques externes...) et placées dans des locaux (ou coffres) sécurisés et distants. Ces copies de sauvegardes devraient être testées régulièrement conformément à la politique de sauvegarde convenue.

9.5.4.c- Journaux systèmes – les « logs »

Les journaux systèmes produits par nos serveurs informatiques permettent la surveillance du contrôle d'accès à nos systèmes et réseaux. Ils permettent de faciliter les investigations ultérieures, et sont en outre également exigés dans le cadre de la collecte de preuve par les autorités juridiques compétentes.

Les journaux systèmes qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant la période légale pour surveiller l'exploitation du système. La politique de gestion des traces du CNRS a fait l'objet d'un document disponible dans l'intranet du CNRS [log cnrs].

Il est important de protéger les serveurs qui conservent les informations journalisées contre les accès non autorisés ou des actes de malveillances qui pourraient s'opposer au maintien de la preuve.

En raison du nombre de serveurs présents dans nos unités, il convient de mettre en œuvre des moyens pour faciliter l'exploitation transversale de ces journaux provenant de multiples serveurs. Par exemple la centralisation des journaux systèmes sur un serveur unique et dédié, permet de concentrer la sécurisation des « logs » sur un seul point d'accès, de mieux réguler la période

d'archivage légal, et surtout de permettre la consultation simultanée des journaux de plusieurs serveurs [journaux systèmes].

9.5.4.d- Synchronisation des horloges

En cas d'analyse des journaux informatiques, pour retracer la chronologie d'un événement ou d'une anomalie, il est essentiel que les horloges des différents systèmes de traitement de l'information (serveurs, routeurs, PC utilisateurs..) de nos entités de recherche soient synchronisées à l'aide d'une source de temps précise et préalablement définie.

9.5.4.e- Sécurité du réseau – Echange des informations – Contrôle d'accès réseau

Les réseaux de nos unités de recherche doivent être gérés et contrôlés de manière adéquate pour garantir leur protection contre des menaces aussi bien externes qu'internes. On veillera surtout à contrôler l'accès physique au réseau, segmenter le réseau local en différents réseaux virtuels et à rendre illisibles notamment les informations en transit, par des moyens de chiffrement des protocoles :

- ***contrôle d'accès réseau :*** il est nécessaire d'empêcher les accès non autorisés aux services qui sont disponibles sur le réseau (partages de dossiers, imprimantes, accès Intranet Web, etc). L'ASR doit s'assurer de ne donner accès qu'aux services pour lesquels les utilisateurs ont spécifiquement reçu une autorisation. Des méthodes d'authentification appropriées doivent donc être utilisées pour contrôler l'accès des utilisateurs distants. Il peut être nécessaire d'avoir recours au standard 802.1x. pour contrôler l'accès aux ports du réseau interne au moyen d'une identification et authentification La mise en place d'annuaires centralisés tels que Active Directory ou LDAP ou encore un serveur Radius représente un élément fondamental pour permettre cette authentification.
- ***cloisonnement des réseaux :*** il est particulièrement efficace de séparer les flux réseau issus des différents services d'information de nos entités. La segmentation du réseau de l'unité en réseaux logiques virtuels (VLAN) est une bonne mesure à prendre pour séparer les flux réseau de différentes entités administratives (le réseau des chercheurs, le réseau des étudiants, le réseau de secrétariats, le réseau des serveurs...). Cette différentiation des flux permet par la suite de leur appliquer des mesures de sécurité différentes. Dans le processus de segmentation du réseau. Il est fortement recommandé de regrouper et d'isoler les services devant être visibles de l'extérieur dans une zone réseau « semi ouverte ».
- ***contrôle du routage réseau*** : le réseau hébergeant le S.I. doit être protégé des tentatives d'accès illicites provenant de l'extérieur comme de l'intérieur de nos entités. Des mesures du routage des réseaux doivent être mises en œuvre afin d'éviter que des connexions réseau non souhaitées ne portent atteinte à la politique de contrôle d'accès des applications métier de nos entités. Les flux d'entrée et de sortie du réseau doivent également être protégés par un ensemble de filtres (« ACL ») qui permettent d'interdire des accès réseau vers des ressources ou des services non contrôlés.

9.5.4.f- Protection des transferts de données : chiffrement

L'objectif des mesures cryptographiques est de protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des algorithmes utilisant des clés de chiffrement. Aussi, il faut les utiliser pour protéger les flux d'information liés à des services sensibles. Par exemple, la messagerie électronique ou les accès intranet ou tout autre service demandant une identification doivent être

protégés de manière adéquate par des protocoles sécurisés reposant sur SSL, comme IMAPS, SSMTP, SASL pour la messagerie ou HTTPS pour le WEB.

Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information devrait être mise en œuvre. Cela revêt un caractère obligatoire pour les données classifiées «sensibles ». On consultera à cet effet le document de recommandations du CNRS en la matière [Chiffrement].

Il est important pour les ASR de connaître le fonctionnement de l'infrastructure de gestion des clés (IGC) et l'utilisation que l'on peut faire des certificats délivrés (signature et chiffrement des messages électroniques, ou encore certification de machines serveurs …).

Dans le cas du CNRS par exemple, l'ASR se rapprochera des Délégations Régionales pour connaître les modalités d'obtention et d'utilisation des certificats électroniques du CNRS, ainsi que celles pour devenir « Autorité d' Enregistrement » (AE) afin de fournir des certificats électroniques aux utilisateurs de son unité. Il est à ce propos nécessaire de connaître l' Autorité d' Enregistrement en place sur la Délégation Régionale. On trouvera de nombreuses documentations à ce sujet sur le site de l'IGC du CNRS, http://igc.services.cnrs.fr .

9.5.4.g- Exigences relatives au contrôle d'accès aux systèmes d'exploitation

Il est du ressort des ASR de maîtriser par des dispositifs techniques ou procéduraux, l'accès à l'information présente dans nos unités. Il est donc nécessaire de mettre en place une politique de contrôle d'accès de manière à empêcher les accès non autorisés aux systèmes d'exploitation.

Une procédure formelle de création (et de suppression) des comptes informatique des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie. Après création des comptes, il est nécessaire de gérer correctement l'attribution et l'utilisation des privilèges.

L'accès aux ressources informatiques ne doit donc être possible qu'après identification et authentification des utilisateurs, et doit être adapté aux droits et aux profils des utilisateurs (chercheurs, administration, enseignement, etc).

L'ASR attribue un identifiant et un mot de passe uniques à chaque utilisateur, et met en place le système d'authentification adéquat, pour vérifier l'identité déclarée par l'utilisateur lors des entrées en session.

Les utilisateurs doivent pouvoir changer leur mot de passe par un processus formel contrôlé de manière à empêcher l'utilisation de mots de passes trop faibles (mots ne figurant pas dans un dictionnaire, et difficiles à retrouver à l'aide de programmes).

Il est important de faire adhérer les utilisateurs à ces mesures qui peuvent paraître contraignantes, mais qui figurent parmi les mesures de base permettant d'assurer la sécurité de l'accès au S.I des entités.

Dans certains contextes (salles d'enseignements, ou applications sensibles...) les sessions inactives devraient être déconnectées après une période d'inactivité définie.

9.5.4.h- Gestion de Parc et des moyens nomades - Cybersurveillance

L'administration des postes de travail de nos unités est normalement placée sous la responsabilité de l'ASR. Selon la réglementation en vigueur actuellement, il a donc toute latitude pour mettre en place des outils de gestion et de surveillance du parc informatique. Ainsi, une

vérification du niveau de sécurité des postes nomades (présence d'un antivirus à jour par exemple) doit être mise en place avant l'accès au réseau local. Les postes de travail et moyens nomades doivent par ailleurs être protégés par des mots de passe robustes.

En cas de télémaintenance sur un PC avec des outils de prise en main à distance tel que VNC, les ASR doivent avertir le propriétaire du poste et respecter la législation.

9.5.4.i- Mesure de l'utilisation des ressources : outils de métrologie

L'utilisation des ressources systèmes ou du réseau doit être surveillée et ajustée au plus près. La sécurité du S.I implique une surveillance de l'utilisation du réseau et des serveurs tout en respectant la réglementation en vigueur (cf bonnes pratiques liées aux aspects juridiques §10). Cela consiste notamment à respecter le principe de proportionnalité qui est d'adapter les moyens de surveillance aux enjeux de sécurité, et d'avoir pour principe d'informer les utilisateurs et les partenaires sur les moyens de surveillance mis en place. Dans le respect de ce cadre l'ASR a toute latitude pour mettre en place divers outils de métrologie réseau et de journalisation des accès aux serveurs.

10- Bonnes pratiques liées aux aspects juridiques du métier d'ASR – respect de la réglementation en vigueur

Le travail des ASR est désormais en prise avec de nombreuses obligations et responsabilités de nature juridique.

Dans le cadre de la protection du S.I, la responsabilité administrative et pénale de la hiérarchie et des ASR peut être recherchée. Il conviendra donc de connaître les principaux règlements en matière de cyber protection (LCEN, informatique et liberté) relatifs à la protection de la propriété intellectuelle, des données relevant de la vie privée (fichier nominatifs), et de suivre attentivement l'évolution des jurisprudences.

Quelles sont les bonnes pratiques dans le contexte des responsabilités juridiques ? Les jurisprudences appliquées ces dernières années ont permis de dessiner un ensemble de comportements et de bonnes pratiques, permettant à l'ASR d'avoir une attitude plus éclairée dans un contexte de faute potentielle dans le S.I.

Une règle fondamentale qui apparaît dans le métier d'ASR depuis la LCEN, est le triptyque « information - contrôle – action ». Dans un contexte de faute, un magistrat jugera si on a : « informé » les utilisateurs, si on a « contrôlé » les ressources mises à défaut, et si on a « agi» dans des délais acceptables pour réparer une faute ou un problème.

10.1- Informer, contrôler, agir

10.1.1- Informer, Conseiller

Les administrateurs sont tenus à une obligation de conseil « renforcé » auprès des utilisateurs d'un système d'information (le conseil « renforcé » s'applique à 3 domaines : nucléaire, chimie risque de type « SEVESO » et informatique) . Les ASR peuvent et doivent donc émettre des alertes (sur des risques connus) ou des mises en garde (sur des risques possibles)... La mise en garde permet de signaler qu'il est possible qu'un problème intervienne. L'alerte permet d'informer d'un problème bien défini et connu (et non hypothétique). La présence de certains mot-clés (alerte, conseil, mise en garde) dans un rapport ou un mail peut avoir un poids utile en cas de contentieux ultérieur.

Il faut informer les responsables légaux, les autorités compétentes ainsi que les utilisateurs par la rédaction de rapports réguliers, ainsi que sur toute situation particulière pouvant mettre en cause la sécurité du S.I. (Cf. § Documentation).

Il est nécessaire d'informer les utilisateurs de la nature des traces qui sont journalisées et archivées sur nos systèmes, ainsi que de leur durée de rétention par l'affichage sur un site web par exemple.

10.1.2- Prouver qu'on a sécurisé

C'est une bonne chose de mettre en œuvre un ensemble de techniques assurant la sécurité informatique, mais encore faut-il pouvoir le prouver. Or, dans nos milieux universitaires et de recherche il y a une faible « culture de l'écrit administratif ». On ne trace pas beaucoup par écrit les actions qui ont été entreprises. Il faut donc pour nous ASR, pour prouver nos actions, montrer qu'on a informé et agi.

Par conséquent, il convient de tracer et documenter nos actions de diverses manières. On retrouve là la nécessité issue des processus de gestion des interventions et de gestion des changements cités dans la première partie de ce document.

Il faut avoir les moyens de donner des preuves de l'information et de la communication qu'on a fourni. Cela peut prendre différentes formes comme par exemple, faire un rapport annuel d'activités, ou tenir la rédaction d' une rubrique « informations » notamment sur la sécurité sur le site Web du laboratoire.

Une rubrique « sécurité » sur un site web peut permettre de retranscrire régulièrement les actions d'information et de contrôles engagées. Les utilisateurs de l'unité doivent bien sûr être informés de l'existence de cette rubrique et de sa mise à jour (Cf. § Documentation).

Il est préférable de garder des preuves électroniques et au besoin écrites de diffusion de l'information. Ces informations seront donc faites par écrit (mail, article web, notes de service..), et pourront comporter certains mots-clés comme « CONSEIL », « MISE EN GARDE », « ALERTE » .

Ces informations peuvent porter par exemple sur certains bulletins d'alerte du CERT ou CERTA qui concernent l'unité, les migrations prévues ou les interruptions de services critiques, ou encore des coupures du réseau avec l'extérieur. On peut y mettre également des statistiques de virus/ spams, débits réseau, infections PC , un bilan d'activité annuel du service, etc.

10.1.3- Contrôler l'activité des systèmes et du réseau

Le contrôle vise la mise en place d'outils de surveillance pour vérifier le bon fonctionnement loyal et proportionné des services offerts.

Depuis la LCEN, le droit des ASR à tracer les activités des services et leur utilisation dans le S.I est total et complet : diagnostic, analyse, contrôle, maintenance préventive, identification des comportements illicites.

Les bonnes pratiques consisteront par exemple à détecter les fonctionnements anormaux par la mise en place d'outils pour :

- centraliser et paramétrer la conservation des journaux systèmes sur la durée maximale légale pour les services demandés,
- obtenir des statistiques sur l'utilisation des services, le débit, les sites consultés, la consultation du site du laboratoire, la place occupée sur les disques, …,
- avoir des remontées d'information en cas de problème avec des sondes d'un système de « monitoring » (Nagios, cacti, Zabbix, etc) par exemple,
- contrôler le contenu du site web. Dans la majorité des cas, les laboratoires éditent et hébergent eux-mêmes leur site web. L'hébergeur n'a pas d'obligation générale de surveillance, mais il a une obligation *spéciale* de surveillance (point de la négligence fautive). Les ASR sont en effet tenus au secret professionnel, mais ont l'obligation de dénoncer des actes délictueux comme les contenus illicites et notamment la pédo-pornographie ou la diffamation. En tant que directeur de la publication, le directeur du laboratoire a une plus grande responsabilité puisqu'il en approuve le contenu.

L'ASR est tenu, comme tout agent de l'État, de dénoncer les contenus illicites dont il constate la présence (ceux qui font l'objet de crimes ou de délits). Il ne faut cependant pas effectuer de destruction de preuve. Il sera conseillé de faire une « copie d'huissier » des fichiers incriminés (sur un support comme une CD-ROM, etc) et de les placer en lieu sûr pour le cas où une enquête ultérieure serait menée.

Une attention particulière sera à observer pour tout ce qui touche aux informations personnelles (contexte de la vie privée résiduelle sur le lieu de travail), tant en terme de diffusion du contenu que de diffusion d'information concernant un contenu suspect.

Il est à rappeler que la remise de documents ou d'informations touchant aux données personnelles ne peuvent être remises qu'à un officier de police judiciaire dûment habilité (en cas de doute, ne pas hésiter à contacter le HFD directement ou via la chaîne organique).

10.1.4- Agir

En cas de crise ou d'urgence, l'ASR a donc le droit d'agir et réagir rapidement pour assurer la continuité du service et dispose du droit de refuser des demandes qui mettraient le S.I. en danger.

En contre partie, il est tenu d'assurer la sécurité système du site (passer les correctifs de sécurité logiciels). Si un correctif de sécurité n'a pas été passé, et qu'il y a eu un incident grave, pour ne pas être responsable, il faudra prouver par exemple qu'il était en vacances, et qu'il n'y avait pas de redondance humaine prévue.

Pour maintenir la continuité des services communs, pour sécuriser (exécuter les patchs,...), en cas d'urgence ou de crise,les principes généraux et fondamentaux du métier d'ASR à retenir sont :

- améliorer la « politique de l'écrit » dans nos unités,
- mettre en place le triptyque Information/Contrôle/Action,
- améliorer la traçabilité.

10.2- Notice légale de site web

La loi pour la confiance dans l'économie numérique du 21 juin 2004 prévoit que les personnes dont l'activité est d'éditer un service de communication au public en ligne mettent des informations à disposition du public :

- nom, prénoms, domicile et numéro de téléphone,s'il s'agit de personnes physiques,
- dénomination, raison sociale et siège social, numéro de téléphone,s'il s'agit de personnes morales,
- nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction,
- nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone de l'hébergeur.

Une notice légale est donc désormais indispensable sur les sites Webs de nos unités. Celle-ci doit indiquer :

- l'exploitant du site : c'est une entité, généralement le laboratoire lui-même,
- l'hébergeur : c'est l'entité qui a le contrôle logique sur le serveur : c'est soit le laboratoire s'il a le contrôle total sur le serveur, soit l'entité qui gère ce serveur (sur lequel le laboratoire a un point d'accès pour mettre à jour son site web),
- le Directeur de la Publication : c'est une personne physique, généralement le Directeur du laboratoire (ou le directeur Général du CNRS).

Dans ce contexte, il est bon de préciser que l'ASR a pour mission d'assurer l'administration système des serveurs, mais ne doit pas être l'éditeur ou le responsable éditorial du site Web de l'établissement.

Si l'ASR est informé d'un contenu illicite, il doit en informer son directeur par écrit et prendre une décision rapide pour sauvegarder les preuves puis ensuite retirer ce contenu. La Loi dit de le supprimer « immédiatement ». Dans les jurisprudences, le délai est généralement de 48h.

10.3- Notion de charte informatique

La charte de bonne utilisation des services informatiques et de l'internet est un document indiquant quels sont les droits et devoirs des utilisateurs. Elle doit être largement diffusée et portée à la connaissance de tous les personnels de l'entité. Une charte acceptée (qu'elle soit signée indépendamment ou annexée au règlement intérieur) est un élément de droit. Elle est assimilée à un contrat et doit donc être comprise pour être valide (ne pas faire signer la charte française à un étudiant étranger qui ne la comprendrait pas). Elle complète un dispositif qui peut être constitué de normes, de plan de continuité d'activité, d'audit, ou d'actions de sensibilisation.

CONTEXTES PERSONNEL ET RELATIONNEL DES ASR

Cette partie traite des pratiques que peut suivre l'ASR en tant qu'individu dans son contexte pour mieux organiser son travail, mieux communiquer au sein de son entité et améliorer ses compétences. On y trouvera donc des méthodes de gestion du temps, des principes pour améliorer la communication entre l'ASR et son environnement (directeur, utilisateurs,..) et des outils pour perfectionner ses compétences par le biais de différents types de formation.

11- La gestion du temps

La nécessité de gérer son temps n'est pas primordiale tant que nous pouvons faire face à l'ensemble de nos tâches « naturellement » dans un temps raisonnable. Si nous avons l'impression que notre charge de travail ne cesse de s'alourdir et que notre méthode « naturelle » d'organisation fonctionne moins bien alors, une réflexion s'impose.

Nous sommes, en effet, soumis a des sollicitations plus ou moins imprévisibles. Notre travail est souvent assujetti à un flot continu de requêtes diverses provenant des utilisateurs qui rentrent en concurrence avec les tâches incontournables d'administration des infrastructures. Il faut donc s'organiser au mieux pour répondre à cette situation et savoir gérer son temps est un des moyens pour y parvenir.

Outre ces demandes et ces incidents dans l'exploitation du parc informatique, nous avons besoin de maintenir nos connaissances concernant la veille technologique. Cela demande de réserver du temps pour tester, évaluer les nouveaux produits, connaître de nouvelles technologies, etc.

Enfin, appliquer une méthode de gestion du temps apporte une aide lors de la rédaction des rapports d'activités. En effet, on peut se référer aux listes de projets, d'actions élémentaires, à l'agenda, à l'échéancier tenus à jour au cours de l'année passée.

Notre objectif est de donner quelques pistes concrètes pour améliorer la gestion du temps dans le métier d'ASR, principalement, à partir de trois sources d'informations qui sont :

- la méthode « Getting Thing Done », de David Allen, plus connue sous l'acronyme GTD [GTD],
- le livre de Thomas Limoncelli « Admin'sys, gérer son temps »[AdminSys].
- le livre de François Delivré « Question de temps » [QuestionTemps]

11.1- Les grands principes de la gestion du temps

La majeure partie du stress naît d'une mauvaise gestion des engagements pris ou acceptés. En effet, si on prend le temps de réfléchir sur les tâches réalisées lors des dernières semaines par exemple, on se rend compte du très grand nombre d'engagements internes pris : cela va des grandes ambitions (projet d'Université Numérique en Régions ou la restructuration du service informatique), jusqu'à des intentions plus modestes (des migrations de services, mise en place de nouveaux serveurs) ou encore banales (remplacer le bloc-notes ou recharger le portable). Prendre conscience de ces divers type de tâches est un pas certain vers une meilleure gestion de son temps.

Un autre point important également est de pouvoir définir à quel niveau de réflexion ou de "profondeur" se situe un projet ou une tâche. Par exemple, un projet reste flou ou une affaire en suspens s'il n'a pas d'objectifs clairs (que veut-on vraiment obtenir ?) et si aucune action concrète n'a été définie. Ce n'est pas quelque chose de négatif en soi. Au contraire, cela correspondant au tout début du projet, au moment ou l'idée émerge tout simplement. Ceci dit, un projet flou est très difficile à planifier puisqu'aucun déroulement n'est défini. C'est un point capital d'autant plus que s'il nous préoccupe excessivement, c'est que soit on n'a pas les moyens pour le régler ou bien on n'a pas de solutions.

La plupart des conflits de priorité à un instant donné entre plusieurs tâches peuvent être résolus par une bonne harmonisation entre les tâches nécessaires (« il faut que ») et celles qu'on aime bien (« j'ai envie de ») [QuestionTemps]. Si nos tâches du type « il faut que » sont trop prépondérantes

par rapport à celles du type « j'ai envie de », cela se traduira par une démotivation de l'ASR. C'est dans notre « j'ai envie de » que se situe la plus grande énergie, la plus grande détermination à agir.

Enfin, nos difficultés pour gérer notre temps viennent aussi du fait d'être victime des ruses de notre mental dont nous n'avons pas nécessairement conscience tels que être systématiquement tenté de sous-estimer le délai d'une tâche, se disperser, la peur des responsabilités, l'hésitation perpétuelle. François Delivré les appellent les « diablotins » dans son livre. Il en recense une dizaine. En prendre conscience, là aussi peut nous aider à améliorer la gestion de notre temps [ResumeQuestionTemps].

11.2- Le schéma du flux de travail ou la technique du cycle

La méthode GTD propose un schéma du flux de travail[résuméGTD] pour apprendre à gérer son temps. L'idée est de libérer son cerveau le plus possible des diverses tâches à effectuer. Si l'esprit est encombré d'une multitude de détails, il ne pourra pas être efficace. Pour se concentrer et éviter d'oublier, le mieux est de coucher sur le papier ou de saisir au clavier tout ce qui nous préoccupe et de centraliser le tout dans une boite d'entrée.

Ensuite pour chaque élément stocké dans cette boite, soit il s'agit d'une information à stocker dans les documents de référence, à jeter ou à noter dans une liste « A faire un jour/peut-être » , soit il s'agit d'un élément qui demande une action.

C'est à ce niveau que se situe le cœur de la méthode : quelle action faut-il entreprendre ? Pour certains éléments, l'action est évidente et facile à réaliser (envoi d'un mail pour poser une question bien définie, ou pour informer). Pour d'autres, le réflexe est de découper en plusieurs actions élémentaires appelées PCAF (« Première Chose A Faire »). Si la PCAF en question ne demande que quelques minutes, alors le mieux est de l'exécuter sur le champ. Sinon, on se demande si on est la personne la mieux placée pour l'exécuter. Selon la réponse, on délègue ou on la reporte dans sa liste de PCAF, en bref : on exécute, on délègue ou on consigne.

En résumé, il est préconisé de maintenir au minimum une liste de projets, une liste de PCAF et un agenda. D'autres catégories sont aussi utiles et expliquées en détail. Les pointeurs sont donnés dans le document « Fiches de Référence » du guide.

A un instant donné de la journée, on est soit dans la réalisation de tâches prédéfinies (liste de PCAF), soit on gère les imprévus, soit on définit son travail (on est dans ce schéma du flux de travail). Prenons quelques minutes au début pour s'observer : n'est-on pas trop souvent dans les imprévus au détriment des autres tâches ?

Une fois cette organisation établie et bien intégrée, il devient naturel de revenir régulièrement sur son planning en particulier pour réaliser un bilan, effacer les tâches réalisées et en ajouter de nouvelles. L'idéal étant le vendredi après-midi pour libérer son esprit pour le week-end parce le travail réalisé dans la semaine est encore bien à l'esprit. Thomas Limoncelli propose la technique du Cycle, similaire à la méthode GTD : il s'agit de consacrer dix à quinze minutes chaque matin pour mettre en place son emploi du temps de la journée, ordonner selon les priorités et les temps d'exécution, suivre le programme, conclure et recommencer le lendemain.

Il est préférable de commencer avec une organisation minimale (avec un papier et un crayon) à laquelle on adhère complètement car on est convaincu que c'est nécessaire et on l'améliore petit à petit pour soi et pour le service informatique.

Voici quelques exemples de différents types d'informations à traiter dans sa boite d'entrée :

- l'information « disque n°xx de la baie scsi est tombé en panne le ../../.. Remplacé le ../../.. après appel au fournisseur, sous garantie ... » est à stocker dans la fiche d'exploitation du matériel.
- « remplacer le contrôleur de domaine Samba » est un projet à noter dans la liste des projets.
- « se remémorer l'actuelle configuration du serveur samba d'après la fiche d'exploitation ou les fiches d'intervention » est une PCAF de même que « lire les nouveautés entre les 2 versions et réfléchir à leur impact par rapport au paramétrage du service effectif dans mon laboratoire ».

11.3- La gestion des projets et des priorités

Il est fréquent chez les ASR d'être débordés par les demandes quotidiennes, généralement courtes et fréquentes occasionnant le report de grands projets initialement prévus (et qui deviennent de plus en plus urgents au fur et à mesure du temps qui passe). Pourquoi ? Une des raisons est que ces projets sont souvent longs et complexes et qu'il est difficile de savoir par ou commencer.

Thomas Limoncelli comme David Allen propose le découpage en sous-projets plus simples et courts. La méthode GTD est plus concrète dans le sens ou elle préconise de définir une première action (appelée PCAF) concrète et d'une durée assez courte.

Pour définir à un moment donné l'action à effectuer, plusieurs modèles sont proposés. Le premier modèle repose sur quatre critères : le contexte, la disponibilité, le niveau d'énergie et la priorité. Ce dernier critère fait appel à son jugement du moment comme par exemple le « facteur d'impact » de l'action. En effet, connaître les attentes des utilisateurs et faire passer un projet riche en conséquences (pour le laboratoire, pour l'image de marque...) avant les projets faciles mais aux conséquences et retombées moindres ou inutiles est un critère important.

Le classement suivant en 4 catégories, de A à D, peut servir à attribuer une priorité. On privilégiera évidemment la catégorie A :

A: une action facile (effort faible) avec un impact important et positif

B: une action difficile (gros effort) avec un impact important et positif

C: une action facile avec un impact superficiel

D: une action difficile et un impact superficiel

Un exemple peut être la demande de mise en place d'un site web pour une conférence organisée dans son laboratoire. Même si cette demande est la dernière dans l'ordre chronologique, elle peut être classée prioritaire grâce à un impact positif et immédiat vis à vis des utilisateurs et de l'extérieur.

Le second modèle repose sur la notion d'échelle, une façon de prendre du recul. Il s'agit de passer d'un état où on est au plus près des actions en cours à celui qui permet d'obtenir une vue d'ensemble correspondant à son plan de vie [GTD] . Cela permet d'exécuter une action de son plan de vie qui ne fait pas partie des actions quotidiennes. Par exemple, prenons le cas d'un ASR qui souhaite approfondir ses connaissances sur le système Linux, qu'il connait très peu étant plutôt compétent sur le système Windows. Ce souhait fait partie de son plan de vie (mutation, …). Si une formation sur Linux se présente, il choisira d'y participer même si c'est pendant une période où de nombreuses tâches sur le parc des machines Windows l'attendent.

11.4- Mieux gérer les interruptions

Un des grands problèmes dans notre travail d'ASR est le grand nombre d'interruptions auxquelles nous sommes confrontés continuellement et qui nous font abandonner des tâches en cours pour les reprendre plus tard.

Ces interruptions incessantes nous font souvent perdre le fil du travail en cours.

Dans la gestion du temps, l'ASR est également parfois son propre ennemi en étant tenté de répondre au flux incessant de courriels qu'il reçoit et en maintenant trop de tâches en cours (trop de fenêtres à l'écran,...).

Il s'agit alors de mieux réagir aux interruptions fréquentes de notre métier (urgences, multiples demandes des utilisateurs, courriel..), et donc d'organiser au mieux son temps et sa liste de tâches avec des méthodes appropriées parmi lesquelles:

- avoir un environnement rangé favorisant la concentration, et diminuant les distractions (ranger l'écran, pas trop de fenêtres ouvertes et d'actions simultanées en même temps)
- connaître son rythme biologique et savoir à quelle heure on est plus disposé pour des activités nécessitant de la concentration
- mettre en place un « bouclier anti-interruptions », avec un système de plages horaires spécifiquement réservées aux demandes des utilisateurs. En dehors de celles-ci, l'ASR peut alors s'isoler, quitter son bureau et avancer sur ses projets plus sereinement.
- face aux multiples demandes des utilisateurs, revenir au schéma du flux de travail cité dans la méthode GTD : déterminer la « première action à faire » (PCAF), l'exécuter, la déléguer ou la consigner puis recommencer.

11.5- Mettre en place des routines et des automatismes

Ces actions régulières que l'on s'impose permettent de mieux structurer ses activités et gérer son temps. On peut citer par exemple :

- planifier systématiquement des rencontres dans son service pour faire le point sur l'état d'avancement de projets (tous les lundis, le planning hebdomadaire du service informatique, tous les premiers lundis de chaque mois, les réunions avec des collègues, etc). On peut élargir cette habitude de programmer des réunions avec son supérieur, voire les utilisateurs (voir le paragraphe suivant sur la communication)
- mettre en place des scripts pour automatiser les sauvegardes, les vérifications sur la place disponible des serveurs, des services en arrêt, etc.
- automatiser l'envoi de mails pour se rappeler les tâches récurrentes mais manuelles : compacter une base de données, éditer le listing mensuel des machines infectées,etc.
- se déplacer systématiquement avec son organiseur, son stylo, ses clés, ses cartes d'accès est aussi une bonne habitude.

11.6- Conclusion

L'idée qui nous incite à penser qu'appliquer une méthode de gestion de temps apporte un travail supplémentaire sans réel bénéfice est très répandue. Cela signifie que la phase

« motivation/intention » n'a pas été traitée en profondeur. En fait, appliquer une telle méthode (qui revient à planifier un projet) ne diminue pas le nombre de tâches que nous avons : ce n'est pas une recette miracle ! Au contraire, elle met en relief, parfois de façon douloureuse, les dysfonctionnements qu'ils proviennent de nous ou non, et va inciter à définir bien clairement les priorités.

Pour maintenir le cap, on doit prendre l'habitude de libérer son esprit, de déterminer les actions nécessaires et les résultats voulus aussitôt qu'une situation se présente, revoir et mettre à jour l'inventaire complet des affaires en suspens. Ne soyons pas étonnés si ces habitudes ne deviennent pas automatiques du jour au lendemain. Soyons patients et apprivoisons-les en douceur !

12- La communication de l'ASR avec ses partenaires

Nous abordons ici les relations avec ce qui, dans ITIL ou la norme ISO20000, est classé sous le terme de "client". En effet, dans un laboratoire de recherche, les ASR doivent bien sûr rendre des comptes et satisfaire des besoins de différentes natures et niveaux. Il y aura donc plusieurs formes de communications adaptées à chaque « catégorie de client » ou de besoin (formes écrites, orales, contractuelles, dialogues, écoutes, etc).

Outre les qualités techniques requises, l'ASR (ou du moins le service informatique) porte également une fonction de communication :

- il a un devoir d'informer, de former et de sensibiliser la Direction et les utilisateurs pour tout ce qui concerne l'utilisation du système informatique, son évolution, ses changements et sa sécurité.
- il a également une obligation de conseil, de recommandation, d'alerte et de mise en garde pour toutes les pratiques ou événements qui pourraient mettre en cause la sécurité ou le fonctionnement normal du S.I.
- enfin il a un rôle dans la relation au quotidien avec les utilisateurs, à travers la prise en compte des multiples demandes d'assistance de leur part.

D'une manière plus générale, un des rôles de l'ASR, est souvent de reformuler en termes de "solutions techniques" ce qu'expriment les utilisateurs (les clients) en termes de besoins fonctionnels ou scientifiques afin de les concrétiser par des évolutions, des investissements ou des modes de fonctionnement.

La communication (dont l'écoute) est donc un élément fondamental dans nos relations avec les utilisateurs/clients, qui va viser d'une part, à comprendre et prendre en compte les besoins et problèmes des utilisateurs de l'unité et d'autre part à conseiller la Direction dans son rôle de responsable de la sécurité du S.I. Enfin une bonne communication permet d'assurer la bonne lisibilité des missions du service au sein de l'entité.

Il s'agira donc de mettre en œuvre les « bonnes pratiques », les bonnes structures organisationnelles pour assurer ces missions de communication récurrentes à l'intérieur de l'unité comme vers l'extérieur.

12.1- La communication relevant de la « politique générale » informatique de l'unité

On est là dans le cadre du suivi d'un schéma directeur qui va fixer les grandes lignes des activités informatiques au cours de l'année, les priorités à traiter, les investissements à réaliser et l'attribution d'un budget de fonctionnement.

Ce type de communication permet de définir et d'améliorer la « lisibilité » du service Informatique au sein du laboratoire, et permet d'afficher les missions du service, son organisation, ses moyens, les priorités à suivre, ses actions et réalisations, etc.

12.1.1- La communication sur les activité du Service Informatique

La Direction est l'élément primordial dans le management de la sécurité de l'information du laboratoire. L'ASR est son conseiller principal. Le Directeur d'unité s'entoure parfois d'une « commission d'utilisateurs » avec laquelle il va valider les choix techniques et budgétaires que l'ASR lui soumet. Voici quelques pistes possibles à adapter à chaque contexte.

12.1.1.a- Commission informatique d'une unité

Une « commission informatique d'utilisateurs » regroupant les principales fonctions de l'entité (chercheurs, enseignants, administratifs..) est une instance qui peut se prêter parfaitement à l'établissement et à la validation d'une politique générale d'un service informatique d'une unité. Ce type d'instance a plusieurs avantages, parmi lesquels :

- de présenter et valider le compte rendu d'activités annuel établi par le service informatique auprès des représentants de l'unité,
- d'examiner et valider le budget demandé par le service informatique,
- de définir les priorités des investissements informatiques que l'ASR propose,
- de définir les besoins en continuité de services (durées acceptables de perte de services ou durées acceptables de service dégradé),
- de définir ce qui est critique dans le fonctionnement du laboratoire afin d'orienter, établir et justifier aux yeux de chacun les priorités d'intervention des ASR,
- d'avoir un retour sur la qualité de service du service informatique et sur l'indice de satisfaction des utilisateurs.

Le statut de cette commission est à définir clairement dès sa constitution. Les actions mises en œuvre par l'ASR sont avant tout prises en accord avec sa direction. Les avis de cette commission peuvent être consultés et pris en compte autant que possible dans ce contexte.

12.1.1.b- Livret d'accueil informatique de l'unité

La rédaction d'un livret/guide d'accueil décrivant les services offerts, et les procédures pour y accéder pour les nouveaux entrants concourent à une bonne lisibilité des services mis en place par le service informatique. Il permet également de se reposer sur un document qui assurera de gagner beaucoup de temps en n'ayant pas à répéter les mêmes choses à chaque personne, tout en affichant un grand professionnalisme. Ce livret d'accueil peut bien entendu être disponible sous sa forme électronique sur le site web de l'unité.

On peut par exemple indiquer dans ce livret d'accueil les principaux services offerts ainsi que les modalités et procédures pour y avoir accès :

- l'architecture en place, ses fonctions et ses limites,
- les demandes d'assistance informatique,
- l'accès et l'usage de la messagerie, la configuration de son logiciel de messagerie avec les adresses des serveurs en fonction,
- le changement de son mot de passe,
- l'échange de fichiers volumineux avec un correspondant extérieur,

- l'espace de stockage en réseau, comment y accéder, les quotas disques disponibles par individu,
- l'accès au service de réseau sans fil, à Eduroam,
- la politique de sauvegardes des données,
- l'accès aux moyens de calcul disponibles dans l'unité,
- la salle libre accès, quels sont les logiciels disponibles et les horaires d'ouverture,
- le service VPN pour accéder de manière sécurisée à ses données depuis l'extérieur du laboratoire,
- etc.

12.1.1.c- Compte rendu d'activités

Le compte rendu d'activités du service informatique est un document de communication. C'est l'élément qui affiche, archive et témoigne des grandes tâches réalisées par le service tout au long de l'année devant les utilisateurs et la Direction. Il est aussi important que ces activités fassent partie du rapport rédigé lors des rapports d'évaluation des autorités de tutelle.

Pour exemple, on pourra y mettre :

- une synthèse du nombre et de la diversité des tâches d'assistances réalisées auprès des utilisateurs, et qui ont été inventoriées par le processus de gestion des interventions. Cela peut par exemple se traduire effectivement dans nos unités par un « système de suivi des demandes » (HelpDesk).
- les extensions ou modifications du réseau, du câblage, du déploiement de wifi,
- les changements et évolutions dans les systèmes d'exploitation,
- les installations de nouveaux services,
- l'état des lieux des serveurs et des systèmes de stockage : quantitatifs (nombres de machines, PC, portables, augmentation par rapport à l'an dernier et nombre de services) et qualitatifs (libellé des services implémentés),
- les problèmes de sécurité qui ont eu lieu et comment y remédier,
- les formations effectuées,
- les études et projets en cours et finalisés,
- etc.

En définitive, il permet de résumer et de présenter au grand jour l'ensemble des activités et des tâches réalisées améliorant, de ce fait la communication et la lisibilité du service informatique.

12.2- La communication avec les utilisateurs

Outre la politique générale définissant les missions et orientations générales du service, les ASR sont au contact permanent et quotidien avec la quasi totalité des personnels d'une unité en traitant leurs demandes d'assistance et les diverses résolutions d'incident.

Sans une organisation rigoureuse et adaptée qui permet d'étaler et planifier les interventions, on est assuré d'une perte de temps, d'un stress quotidien, et du sentiment d'être débordé en permanence.

Quelles sont les bonnes pratiques dans ce domaine ? Il s'agit de faire connaître aux utilisateurs les moyens et les procédures mis en place pour satisfaire leurs demandes, comme par exemple :

- un Système de Suivi de Demande ,
- un site Web intranet propre au service informatique.

Il est nécessaire de bien expliquer quelles sont les procédures (où, qui et comment) à suivre en cas de problème et vérifier régulièrement la qualité de la communication (commission d'utilisateurs), comme par exemple un mode d'emploi clair pour trouver la bonne documentation en ligne sur le site Web. On privilégiera les outils et procédures de communication généraux qui serviront à former le plus grand nombre (1 vers n), plutôt que de s'adresser n fois à une seule personne (1 vers 1). La communication avec les utilisateurs pourra s'effectuer au moyen de formations internes et par la mise à disposition d'informations au moyen du système documentaire mis en place.

12.2.1- Relation « 1 vers 1 »

C'est dans ce type de communication qu'il faut veiller à insister sur l'écoute pour détecter les besoins sous-jacents et les reformuler en termes opérationnels.

Il est nécessaire pour l'ASR de prendre en compte toutes les demandes d'intervention des utilisateurs et d'accuser réception de leurs demandes en leur accordant de l'attention nécessaire. On évitera une « non prise en compte » de la demande ou une « réaction silencieuse », et on privilégiera les demandes des utilisateurs qui auront suivi les consignes et procédures mises en place par le service informatique et auront inscrit leur demande sur l'outil de suivi de demandes. Autant que faire se peut, on évitera le vocabulaire du métier afin d'être compris par un utilisateur perdu qui a du mal à exprimer sa demande.

A cet effet l'ASR a le choix entre notifier, enregistrer la demande dans le « HelpDesk » [GPLI][RT] Esup-Portail] pour un traitement ultérieur, ou aiguiller les utilisateurs vers le bon interlocuteur. Dans les deux cas la prise en charge de la demande est un gage de professionnalisme et de qualité de service.

Cet archivage des demandes des utilisateurs dans un « HelpDesk »[HelpDesk] permet à l'ASR de se donner la possibilité de planifier et ordonnancer son exécution, plutôt que d'être ballotté par les interruptions incessantes. Un « HelpDesk » permet également de déléguer une requête à d'autres ASR. L'utilisateur voit par qui sa demande est prise en compte et peut suivre l'état d'avancement de sa réalisation.

12.2.2- Relation « 1 vers n »

La diffusion d'informations sur les « événements en cours », par exemple à partir d'un site Web spécifique du service informatique pourra permettre d'informer les utilisateurs sur :

- les projets en cours : un service wifi qui sera installé à telle date,...
- les évolutions prévues ou en cours sur tel ou tel système : changement du serveur web , prévu à telle date,...
- les nouveautés qui ont été installées : un agenda collaboratif va être installé,...
- les changements de configuration de certains services : en raison de nombreux problèmes de sécurité les connexions ssh se feront désormais sur le port 2324,l'organisation de formations internes regroupant plusieurs utilisateurs sur, par exemple, « l'utilisation de SPIP », ou le « paramétrage de thunderbird »,...

12.2.3- Prise en compte de la satisfaction des utilisateurs

L'analyse de la satisfaction des utilisateurs est à l'origine du processus d'amélioration continue (Roue de Deming, PDCA que l'on retrouve dans ITIL et la norme ISO-20000). C'est une étape fondamentale de la qualité de service dans laquelle on doit vérifier la qualité du service rendu aux utilisateurs, s'assurer qu'elle répond bien aux besoins et à la demande, et l'améliorer le cas échéant.

Dans nos structures, cela pourrait se concrétiser de manière informelle par des rencontres planifiées avec les utilisateurs : mini-séminaires, cafés informatiques, etc) ou encore de manière plus officielle et formelle par des « commissions informatiques » d'unités avec la Direction et les utilisateurs pour faire remonter un niveau de satisfaction.

12.2.4- La communication au sein du service informatique

Enfin, outre la communication dirigée vers les utilisateurs (« client ») de l'unité, il est également nécessaire de bien communiquer au sein même du service Informatique. Dans ce cadre là, les bonnes pratiques quand l'effectif du service le permet, sont :

- de mettre en place des réunions de service régulières. Ces réunions dont la fréquence est à déterminer (quotidiennes ?, hebdomadaires ?...) permettent de passer en revue les actions et les problèmes en cours, de savoir qui s'occupe de quel projet pour quelle échéance, de savoir quelles sont les priorités et les objectifs... Ces réunions peuvent aussi permettre d'élaborer un planning qui servira de « bouclier anti-interruption » en assignant telle ou telle personne à temps plein sur une action pendant que les autres prennent en charge les demandes et problèmes quotidiens des utilisateurs.
- mettre en place et tenir à jour un système documentaire (cf chapitre 8) permettant d'échanger toute la connaissance au sein du service en l'absence des autres membres.

12.3- Communication, collaboration avec les partenaires extérieurs

Le milieu de la recherche scientifique est par principe très ouvert à d'autres partenaires extérieurs. Il est nécessaire de mettre en place une communication appropriée auprès de ce public particulier externe à nos unités. En effet, d'une part nos unités sont souvent hébergées par des tutelles différentes, et d'autre part, elles sont amenées à travailler avec des partenaires industriels.

Nos unités partagent souvent leur environnement technique avec d'autres partenaires, si bien que les limites du S.I peuvent être floues ou mal définies. Il est donc nécessaire de mettre en place une large ouverture et communication avec ces partenaires comme par exemple :

- mettre en place une coordination avec les autres tutelles. En cas d'incidents de sécurité, notamment il convient d'informer et de se concerter avec les autres tutelles.
- intégrer des groupes de travail avec les tutelles qui hébergent des unités de recherche, notamment pour des projets communs de déploiements et de sécurisation du S.I.
- prendre en compte et respecter les règles de sécurité d'un partenaire lors de la connexion à son S.I. par des moyens nomades du CNRS.

Les circuits de communication de l'ASR sont également tournés vers l'extérieur. Il collabore étroitement avec diverses instances extérieures et avec les autorités compétentes relevant de sa

tutelle ou de son environnement professionnel. On aura soin d'avoir régulièrement des échanges ou des réunions avec par exemple :

- la Direction du S.I (le Directeur de l'unité),
- le CRI de l'université ou du site hébergeur,
- la chaîne fonctionnelle de sécurité mise en place par la PSSI de l'établissement,
- le RSSI local l'Université, s'il existe ou son équivalent le plus "proche",
- la CNIL ou toute autre autorité judiciaire qui pourrait requérir l'information,
- les réseaux métiers locaux.

12.3.1 Les relations avec les fournisseurs et les achats

De nombreux ASR, lorsqu'ils occupent des fonctions de gestion de service sont également amenés à manipuler l'argent public de leur entité, pour le fonctionnement et pour les investissements du service informatique. Ces investissements peuvent, bien souvent, être très onéreux (système de sauvegardes, système de baies de disques SAN ou NAS, cluster de calcul …), et les ASR devront être particulièrement vigilants sur le plan technique et budgétaire pour acquérir les matériels aux meilleurs coûts.

De nos jours, l'ASR doit alors également souvent s'investir et avoir des compétences dans la rédaction et la passation des marchés publics (CCTP, CCAP, MAPA, PUMA...). Il doit, par ailleurs, avoir des qualités relatiionnelles pour contacter les fournisseurs, obtenir des démonstrations, négocier des prix et savoir choisir entre des offres partiellement comparables.

13- Recommandations sur les compétences

13.1- Objectifs

C'est un lieu commun de rappeler que l'informatique est un des domaines où l'évolution des techniques a été une des plus rapides ces dernières années. Les techniques ne sont d'ailleurs pas les seules à évoluer : les contextes d'exercice de nos métiers changent. Les notions techniques des utilisateurs ne sont plus les mêmes qu'il y a 10 ans, leurs rapports à l'informatique s'est modifié et notre communication doit s'y adapter.

Dans le contexte d'une unité de recherche, le métier d'informaticien couvre des domaines très étendus qui concernent l'administration des systèmes et réseaux, l'assistance aux utilisateurs en bureautique, en passant parfois par la programmation, la mise au point de processus d'acquisition expérimentaux ou encore la gestion et de l'optimisation de grappes de calcul (domaine de l'informatique scientifique).

L'ASR, souvent isolé, doit faire preuve de compétences et de savoir-faire dans un grand nombre de domaines simplement pour répondre aux diverses missions qui lui sont confiées, aux utilisateurs et de par son métier.

Outre l'évolution des techniques, les matériels et les logiciels arrivent également vite à obsolescence, en quelques années tout au plus. Des compétences nouvelles sont alors nécessaires pour apprécier et choisir les outils qui vont correspondre aux besoins des utilisateurs, souvent à l'initiative de l'ASR. Le taux de renouvellement étant ce qu'il est (faible en général), il s'agit de prévoir l'utilisation réaliste de ces outils jusqu'à leur terme, en tâchant d'extrapoler raisonnablement leurs évolutions.

De l'assistance utilisateur à l'expression des besoins, de la présentation des choix techniques ou organisationnels aux formations à l'utilisation des outils mis en place, l'ASR doit donc aussi acquérir des compétences diversifiées, allant de la technique aux produits disponibles en passant par la communication pour s'adapter à ses interlocuteurs internes ou externes. Par exemple, défendre ses choix et son budget vis à vis de sa Direction ; savoir gérer les conflits et les priorités (importance de l'aspect "humain" de ses relations). Des formations spécifiques existent dans ces domaines.

Il est crucial que l'ASR se tienne constamment à jour dans le maintien, l'amélioration et l'évolution de ses compétences, de ses connaissances et savoir-faire.

- De quels moyens dispose-t-il pour cela ?
- Dans quel contexte doit-il évoluer pour rester au niveau des exigences requises par sa fonction ?

C'est ce que nous proposons de cerner dans ce chapitre en présentant différents aspects de la « mise-à-niveau » des compétences.

Nous allons proposer quatre voies complémentaires permettant à l'ASR de ne pas être dépassé par les évolutions technologiques :

- l'auto-formation,
- la formation continue,
- la veille technologique,

- les relations métier.

13.2- L'auto-formation

Installer un nouveau système sur une machine de test, valider le paramétrage d'une configuration, ... faire soi-même expérimentalement « sur le tas » sont des manières de progresser et d'acquérir des connaissances et un savoir-faire nouveau.

Toutefois, une bonne pratique va consister à « formaliser » ces nouvelles connaissances : noter et conserver la trace réutilisable de ses expérimentations (sous forme de notes écrites ou de documentations).

Trouver des conseils auprès de collègues dont on sait qu'ils ont une expérience vécue dans un domaine, qu'ils ont eu à choisir une solution parmi l'offre du marché et transmettre en retour ses solutions concrètes permet de capitaliser un savoir-faire collectif.

Il s'agit ici non seulement de ne pas perdre de temps en réitérant les écueils que d'autres ont déjà éprouvés, mais aussi de permettre d'aller plus loin et de partager cette expérience. C'est de la valeur ajoutée à l'expérience des autres.

Avoir à disposition un PC de test, voire une machine virtuelle, pour tester évaluer un nouveau système ou un nouveau service est une manière d'apprendre les nouvelles fonctionnalités et d'acquérir un savoir-faire mais cela nécessite souvent de s'appuyer sur des expériences de collègues ou d'homologues pour valider sa démarche.

S'auto-former sur internet, avec des articles ou des ouvrages de librairies est aussi, bien sûr, une source d'acquisition et d'approfondissement de compétences importantes.

13.3- La formation professionnelle (ex. formation continue)

Trois niveaux sont à considérer en termes de formation :

- l'adaptation au poste,
- l'évolution du métier,
- l'acquisition de nouvelles compétences.

Nos tutelles, conscientes de la nécessité de maintenir les compétences tant techniques que relationnelles voire organisationnelles, disposent de structures de formation financées annuellement :

- chaque délégation régionale CNRS dispose d'un Bureau de Formation Permanente animé par un ou plusieurs conseillers qui coordonnent des correspondants formation dans les unités,
- chaque université a aussi un service de formation avec un correspondant dans chaque département d'enseignement ou de recherche,
- il en est de même dans d'autres EPST ou structures de recherche.

L'interlocuteur sera soit le correspondant formation de son unité, s'il existe, soit le correspondant formation de sa délégation régionale, de son université ou de sa tutelle.

Pour le CNRS par exemple, plusieurs types de formations sont accessibles :

- les formations réalisées à l'initiative des régions, dont le catalogue et les annonces sont en général accessibles sur la site de la Délégation,
- les formations organisées à l'initiative d'autres unités via leur Plan de Formation d'Unité (PFU) et annoncées via le Bureau de Formation,
- les formations nationales dont les « Actions Nationales à Gestion Déconcentrées » (ANGD).

Il est absolument nécessaire à l'ASR de prévoir et de définir des objectifs de formation chaque année. Il devrait être aidé dans cette tâche par son correspondant formation pour la formulation de la demande.

Le Plan de Formation de son unité est le cadre adapté à ces demandes émises par ses membres.

Le personnel CNRS a aussi la possibilité de demander un Plan Individuel de Formation (PIF) afin d'entreprendre sur une période plus longue une formation qualifiante ; il pourra alors bénéficier d'une organisation de son temps de travail en accord avec sa Direction lui permettant de suivre ce cursus.

Élaborer un plan de formation personnel nécessite de connaître ses manques par rapport à l'état de l'art et des avancées technologiques dans le domaine des systèmes et réseau, autant que par rapport à ses besoins propres.

Il peut inclure notamment des formations personnelles (apprentissage de langue étrangère, apprendre à gérer son temps, apprendre à communiquer en public, etc).

On pourra aussi se référer aux fiches d'emploi-type dans l'observatoire des métiers pour apprécier ce qui est demandé et compléter ce qu'on doit acquérir pour être plus efficace et faire évoluer sa mission en faisant des propositions à son unité.

13.4- La veille technologique

Elle permet de se faire une idée des évolutions en cours dans son domaine et d'être en mesure d'anticiper pour proposer des modifications de structures au sein de son unité.

Plusieurs méthodes complémentaires sont accessibles :

- s'abonner à des revues techniques spécialisées ou généralistes du domaine,
- s'abonner à des lettres de « news » techniques,
- assister à des séminaires proposés par les constructeurs ou les fournisseurs,
- participer à des congrès techniques nationaux (par exemple [JRES]) ou des salons techniques, des journées thématiques,
- consulter des sites spécialisés sur internet.

13.5- Les relations de métier

Si l'ASR est souvent isolé dans son unité eu égard à son secteur d'activité, il ne l'est certes pas à l'échelle régionale ou nationale. C'est ce qui a motivé la création de moyens pour mettre en relation les personnes exerçant le même métier ou des métiers proches.

Les services rendus par les ASR ont souvent beaucoup de points communs d'une unité à l'autre, même si les utilisateurs ont acquis des méthodes ou des outils parfois très différents. Il est donc utile d'avoir une liste de contacts, de collègues avec leurs compétences/expériences particulières.

Plusieurs moyens sont disponibles pour enrichir de telles listes : c'est un des buts des réseaux régionaux d'ASR que de partager les connaissances, d'identifier les compétences autour de soi et plus loin si l'on ne trouve pas de réponse à proximité. De nombreuses listes thématiques de messagerie ont été créées au niveau national à l'initiative de l'UREC, du CRU, mais aussi dans les Universités, les campus, etc. Il importe de connaître les listes techniques nationales ou régionales qui permettront d'acquérir de l'information en temps réel. Des serveurs de listes disponibles dans nos communautés peuvent être un bon point de départ :

- serveur de listes du CRU [CRU],
- serveurs de liste du CNRS [CNRSlist],

Les communications entre collègues ASR permettent le partage des connaissances, la capitalisation globale des savoir-faire. L'un aura expérimenté une solution et pourra préciser les difficultés et les risques pour ceux qui comptent la mettre en place.

Trois outils sont disponibles :

- les listes de diffusion : envoyer/recevoir des mails à une communauté thématique,
- les réseaux de métiers : rencontres, exposés, organisation de formations,
- les colloques spécialisés : des journées thématiques organisées tout au long de l'année.

On pourra se référer aux réseaux de métier de la Mission Ressources et Compétences Technologiques (MRCT) du CNRS qui regroupe les réseaux de métiers.

- Le site de la MRCT [MRCT],

Et en particulier à la fédération des réseaux d'ASR : RESINFO

- le site de RESINFO [RESINFO],

Ainsi qu'au site de l'UREC [UREC] pour le CNRS et au CRU [CRU] pour les Universités.

En résumé il peut être utile de tenir à jour un « agenda » qui recense les différentes ressources disponibles dans son environnement selon le modèle ci-dessous :

Type de formation	Type d'information
auto-formation	liste de collègues avec compétences liste de sites internet
formation continue	interlocuteur local interlocuteur délégation interlocuteur université plan de formation
veille technologique	revues lettres de « news » liste de sites séminaires

	congrès
relations de métier	listes de diffusion réseau régional journées thématiques sites de fiches techniques

CONCLUSION

L'ambition de ce guide est de fournir aux ASR quelques principes de base dans l'organisation de leur travail quotidien et de formaliser un ensemble de comportements qui font consensus dans la communauté des ASR.

Comme M. Jourdain faisait de la prose sans le savoir, chacun de nous n'a, bien sûr, pas attendu la sortie des normes ISO, sur lesquelles nous nous sommes appuyées dans ce guide, pour mettre en place certains principes d'organisation de service et des outils afin d'assurer le bon fonctionnement et la sécurité de nos infrastructures informatiques.

Cependant nous avons utilisé les normes ISO-20000 et ISO-27001, dans l'optique générale de donner un cadre référentiel à nos pratiques de terrain, ce qui permet de rendre compte de la meilleure façon, de nos activités et qui contribue, à terme, à améliorer la qualité du service.

Attention : comme il a été dit dans l'introduction et rappelé à plusieurs endroits dans divers chapitres, ce guide n'a pas la prétention d'apporter des solutions "magiques" à nos difficultés de travail mais plutôt de donner des pistes pour mieux s'organiser.

Nous pouvons néanmoins suggérer une approche pragmatique qui consiste, non pas à chercher à systématiquement tout remettre à plat d'emblée dans nos méthodes de travail, mais à tenter, par exemple quand un nouveau projet ou service est à mettre en place, d'appliquer la méthodologie décrite pour le concevoir et passer à la phase opérationnelle.

L'important est de prendre en compte le contexte spécifique de notre environnement avec les moyens dont nous disposons et d'y adapter de manière graduée ces "Bonnes Pratiques".

En rappel et en conclusion, vous trouverez ci-après une synthèse des points importants de ce guide.

Un cadre général : promouvoir une Démarche Qualité

Ce Guide des Bonnes Pratiques, est en effet un document où l'on a tenté de recenser la grande majorité des spécificités du métier d'ASR. Il a été en partie motivé par le fait que les conditions d'exercice du métier d'ASR, dans nos milieux académiques, ne sont pas explicitées dans les fiches métiers qui décrivent les différents postes.

Il nous a donc semblé indispensable, dans le contexte actuel, d'élaborer un corpus de bonnes pratiques d'administration qui contribue à rendre plus «lisibles», vis à vis de nos Directions, de nos tutelles et de nos utilisateurs/clients, les missions du métier, l'organisation et la technicité mis en œuvre au sein de nos services.

Il est bon de rappeler que la référence à une Démarche Qualité va devenir maintenant d'actualité dans le fonctionnement des entités de recherche et d'enseignement, elle a donc été une des lignes directrices mise en avant dans les domaines importants que nous avons traités et dont nous reprenons les points essentiels ci-dessous.

- **La fourniture de services, mission de base de l'ASR**

Tout ce qui concerne la «fourniture de service», dans le domaine de l'informatique et des réseaux et plus largement du S.I est la préoccupation principale du métier d'ASR. Mettre en œuvre

une continuité de services et les conditions de la préservation des données produites par les utilisateurs nécessitent une bonne organisation du travail.

Outre la possibilité de pouvoir améliorer d'une manière continue le service rendu ce guide apporte des clés de base pour mieux structurer le service fourni et, rappelons-le, le faire connaître au mieux par nos Directions, nos tutelles et nos utilisateurs/clients.

- **La sécurité du S.I**

Parmi les points importants à prendre en compte dans les pratiques des ASR figure la sécurité de nos infrastructures informatiques et du S.I.

Cette sécurisation fait partie de nos préoccupations quotidiennes car elle est au cœur du fonctionnement des structures de recherche et d'enseignement. Sa mise en œuvre, malgré des contraintes réglementaires différentes d'une tutelle à l'autre, peut être réalisée grâce à des bonnes pratiques communes que nous avons replacées dans le cadre normatif ISO-27001. Il nous donc a paru indispensable de dégager les principales procédures indispensables à la sécurisation de nos infrastructures.

D'autre part, notre métier, vu sa place névralgique dans la gestion des flux d'informations, touche largement à de nombreuses données à caractère confidentiel et nous avons insisté sur les pratiques de base pour prendre connaissance et suivre les nombreuses évolutions du contexte juridique dans lequel nous évoluons et qui touchent le métier d'ASR.

- **Communication, gestion du temps et relations humaines**

Un autre point important à retenir dans ce guide est la présentation de pistes de bonnes pratiques et conseils pour gérer au mieux les relations humaines avec nos différents partenaires. Le métier d'ASR comporte en effet une forte part de gestion du comportement personnel et de relations publiques et humaines. Nous avons abordé ces différents aspects qui constituent le quotidien des ASR.

D'autre part, l'ASR doit faire face à l'accroissement des demandes de service, répondre aux urgences, tout en assurant la gestion quotidienne et programmer la mise en place de nouveaux services. Il nous faut pour cela de bonnes pratiques de gestion du temps pour organiser les journées et semaines de travail afin de planifier au mieux nos actions. Pour ce faire, nous nous sommes appuyés sur les ouvrages et méthodes connus afin de dégager des méthodes d'organisation du temps.

- **Veille technologique et de formation continue**

Enfin, nous avons terminé en insistant sur le fait qu'il paraît indispensable de penser aussi à intégrer dans notre travail le temps nécessaire à la mise à jour de nos propres connaissances en utilisant largement la formation professionnelle, et les journées organisées par les réseaux métiers ou structures locales des établissements.

Notre métier utilise des matériels et concepts en évolution rapide et notre capacité d'adaptation est, bien sûr, liée à notre capacité à suivre au plus près les évolutions technologiques en cours. La nécessité de se former et d'assurer une veille technologique est donc essentielle.

Quelques autres pistes pour continuer

Nous insistons sur le fait que le fil conducteur de l'ensemble des méthodes abordées est "l'écrit". En effet, que ce soit pour la formalisation des procédures, la documentation, la communication, les rapports d'activités, la gestion de parc, la configuration des équipements, la gestion des traces…, il est indispensable de consigner par écrit (quel que soit le média) ces

informations afin qu'elles soient, confidentielles ou non, transmissibles ou consultables et si besoin partagées.

Par ailleurs, si l'on se réfère au contexte de mutualisation des moyens tant matériels qu'humains qui concerne directement notre métier (par exemple recomposition de laboratoire ou d'équipe de recherche, regroupement de services communs au sein d'un campus, ...), il devient en effet indispensable de travailler avec des outils qui nous permettent une adaptabilité rapide tant des méthodes de travail que des solutions à mettre en œuvre. Ce qui a été proposé dans ce guide ne peut que faciliter la transposition de solutions d'un contexte à un autre et surtout permettre à l'ASR de ne pas avoir à «réinventer la roue» s'il doit travailler dans des cadres différents.

Ce guide est une base qui se veut évolutive, nul doute que nous aurons besoin d'y revenir pour le modifier et le faire évoluer dans les années qui viennent. Le questionnaire ci-joint, à but de bilan/ évaluation interne, en est un prolongement ; utilisez-le périodiquement pour faire le point dans vos activités ou faire des propositions d'amélioration pour la collectivité.

La fédération de réseau de métier RESINFO et les réseaux régionaux ou thématiques qui le constituent sont en effet une des possibilités pour partager vos expériences.

Cette nécessité d'échange de pratique est une "piste" importante à retenir pour donner une suite à ce guide, le maintenir à jour et pouvoir répondre d'une manière efficace à nos missions.

Il revient donc à chacun de nous de l'enrichir et de le faire évoluer par l'apport de nos "bonnes pratiques" quotidiennes mises à l'épreuve des différentes situations d'exercice de notre métier. Toute participation est à cet effet la bienvenue!

Donc à bientôt !

Le contact pour le Guide des Bonnes Pratiques est gbp@listes.resinfo.org

ANNEXE 1 : QUESTIONNAIRE D'AUTO-EVALUATION A USAGE INTERNE

Remerciements: ce questionnaire a été élaboré initialement pour une étude similaire sur les bonnes pratiques des ASR au sein de l'IN2P3 par *J-M Barbet*, et adapté à l'objet de notre guide.

Il est proposé dans le but de permettre à l'ASR de faire le point sur ses pratiques et sur l'état des différents services existants au sein de sa structure.

Il reprend globalement la classification inspirée de la norme ISO exposée dans le guide. Il peut servir à mettre en évidence des aspects à traiter en priorité, se fixer des objectifs, ou réfléchir sur des possibilité de réorganisation du service fourni.

Un exemple d'utilisation de ce questionnaire pourrait être de le refaire à intervalle régulier (chaque année) pour constater ce qui a évolué depuis le bilan précédent, et se fixer de nouveaux objectifs... Une manière comme une autre de mettre en place un plan « PDCA » ... .

1) Recueil des besoins des utilisateurs

- Comment prenez-vous connaissance des besoins des utilisateurs ?
- Vous arrive-t-il d'avoir à les reformuler pour les traduire en service opérationnel ?
- Le recueil des besoins est-il une démarche formalisée ?
- Organisez-vous des réunions avec les utilisateurs dans ce but ? (fréquence, fréquentation)
- Certaines demandes font-elles l'objet d'une négociation et si oui, comment procédez-vous (arguments, exigences, etc.) ?
- Qui arbitre en cas de désaccord, de difficulté ou de conflit sur la définition des besoins ?

2) Gestion des “actifs”- Gestion des configurations

On appelle "actifs" l'ensemble des biens matériels ou immatériels auxquels on peut ajouter des éléments de configuration.
Une première liste non exhaustive pourrait être :

- postes de travail, serveurs, imprimantes, autres périphériques, logiciels, licences,
- consommables, adresses réseau, comptes informatiques, prises réseau, commandes, contrats,...

Disposez-vous d'un système d'enregistrement ou de gestion pour des éléments de la liste ci-dessus ?

- si oui, quelle forme ce système revêt-il ? Outil maison ou commercial ?
- si outil maison : est-ce distribuable à d'autres établissements ?
  - Est-ce basé sur un SGBD ? Lequel ?

- quels sont les éléments gérés par votre outil ?
- utilisez-vous un ou des outils d'inventaire automatique ?
    - Si oui, lesquels ?

3) Gestion des changements et documentation interne au service

- Est-ce que vous enregistrez les événements suivants ? : *indiquez si c'est systématique et pour quelles classes de machines : serveurs, postes fixes, nomades*
    - ajout/suppression de logiciels
    - modifications de configuration
    - correction de problème et de défaut

- Sur quels outils vous appuyez-vous pour ces enregistrements ?
    - logiciels de gestion de conf : CVS, subversion, Trac ?
    - journaux de bord manuels, électroniques ?
    - autres méthodes
- Comment se fait le partage des connaissances au sein de l'équipe des ASRs (si c'est le cas) ?
- Disposez-vous de procédures écrites pour certaines tâches ? Si oui, lesquelles ?

- Comment est organisé la gestion du temps dans le service (si vous travaillez à plusieurs) :
    - Y a t-il des réunions hebdomadaires fixes pour faire le point ?
    - Avez vous mis en place une définition des plages horaires pour les utilisateurs avec un bouclier “anti-interruption”?
- Utilisez-vous un outil ou une méthode de gestion des priorités ?
- Utilisez-vous des outils de gestion de projets? Lesquels? des tâches récurrentes?
- Utilisez-vous des agendas partagés? Lesquels?

4) Documentation pour les utilisateurs, Communication

- Quels sont les principaux éléments couverts par votre documentation ?
- Mettez-vous de la documentation à disposition des utilisateurs ?
    - Si oui, de quelle manière et avec quels outils ?
- Avez-vous des méthodes pour gérer l'obsolescence et l'évolution de cette documentation ?
- Disposez-vous d'une page Web réservée au service (interne ou externe) ?
- Comment les utilisateurs sont-ils tenus au courant de la vie du S.I
    - évolutions, arrêts pour maintenance, incidents, etc.

5) Gestion des demandes des utilisateurs – gestion des incidents

- Disposez-vous d'un outil de gestion et de suivi des demandes des utilisateurs ? Si oui, comment se fait l'affectation des tickets aux personnes chargées de leur prise en charge ?
    - Comment se fait le suivi des tickets ?

- Disposez-vous d'un outil de recherche dans le corpus des tickets résolus ?
- Qui arbitre les priorités et sur quels critères en cas de file d'attente importante ?

6) Surveillance et détection des problèmes – gestion des problèmes

(S'il s'agit d'outils internes, précisez les fonctionnalités générales).

- Disposez-vous de systèmes de détection de sinistres ou de conditions environnementales dégradées ? *(inondation, incendie, élévation de température,...)*
- Disposez-vous de systèmes d'alerte pour des événements susceptibles de compromettre la sécurité logique des équipements ou des données (intrusion, perte/modification de données, virus, etc.) ?
- Disposez-vous de systèmes de surveillance et d'alerte permettant de détecter les problèmes pour les services importants ?
- Quels services, quels outils, quel mécanisme d'alerte ?
- Disposez-vous d'un système de centralisation des journaux systèmes ? D'un système d'analyse de ces journaux ?

7) Gestion de la continuité de service

- Avez vous mis en place des systèmes “haute disponibilité” pour assurer une redondance ? Lesquels et sur quel service? La commutation est-elle automatique, semi-automatique, manuelle ?
- Avez vous mis en place des systèmes de répartition de charge ? Pour quels services ? Lesquels ?
- Avez vous mis en place un plan de reprise d'activités ? Sur quels services? En quoi consiste t-il?
- Quel système de sécurisation et de sauvegarde des données avez vous mis en place ?
- Pratiquez-vous un étalement des congés du personnel du service informatique ?
- Qui peut redémarrer (et comment) les services critiques en cas d'absence de votre part ?

8) Gestion financière

- Rédigez-vous une demande annuelle de moyens financiers auprès de la direction ou des équipes de recherche ?
- Comment vous sont attribués les crédits nécessaires à cette demande ?
- Est-ce une discussion avec la direction et/ou les équipes de recherches ?
- Participez-vous au montage des dossiers CPER, ANR, ... ?

9) Formation

- Avez-vous participé à des stages de formation pendant l'année ?
  - Si non pourquoi ?
- Qu'avez-vous noté comme évolutions prévisibles de solutions matérielles et/ou logicielles qui nécessiteraient une formation pour une mise en œuvre ?
- Faites-vous partie de réseaux métiers régionaux d'ASR ?

10) Sécurité et réglementation

- Prenez-vous en compte les recommandations relatives à la réglementation en vigueur dans le métier d'ASR ou Pensez-vous avoir une bonne prise en compte de la réglementation en vigueur et des actions que nous imposent les jurisprudences rendues récemment ? :

  - gestion des traces informatiques,
  - protection des fichiers nominatifs,
  - notice légale de site web,
  - protection des données, …

Quelles sont les principales actions que vous avez mises en place pour prendre en compte les éléments de sécurité que préconise la PSSI de votre /vos tutelle(s) ? : chiffrement, destruction/effacement des supports magnétiques avant mise au rebut,...

11) Divers

- Participez-vous à la rédaction du rapport d'activité (chapitre spécifique au service) ?
- Disposez-vous d'une page Web réservée au service (interne ou externe) ?
- Etes-vous sensibilisés à la réduction de la consommation électrique de nos équipements informatiques et à celle de consommables informatiques?
- Si oui, qu'avez-vous mis en place (virtualisation, arrêt automatique des machines après inactivité,...).
- Quels conseils donnez-vous aux utilisateurs dans ce sens ?

ANNEXE 2 : FICHES DE REFERENCES

Guide de bonnes pratiques organisationnelles

pour les Administrateurs Systèmes et Réseaux

dans les unités de recherche.

Nous avons répertorié ici un certain nombre d'outils logiciels essentiellement issus du monde « openSource », et de références bibliographiques pouvant illustrer et être utilisés dans les différents chapitres de ce guide des bonnes pratiques.

Introduction

- Productions antérieures de groupe de travail de RESINFO :
  - **[SiLabo] :** http://www.resinfo.org/spip.php?article11 : aider le responsable chargé du S.I d'un laboratoire à identifier et à spécifier les services rendus, actuels ou futurs, ainsi que les ressources nécessaires
  - **[EcoInfo]** : http://www.ecoinfo.cnrs.fr/ : Les activités de ce groupe de travail se concentrent autour des problématiques de la consommation énergétique et de la pollution liées à l'utilisation et au développement de l'outil informatique.
  - **[PSSI CNRS]** : http://www.sg.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/PSSI-V1.pdf : Politique de sécurité du S.I du CNRS
  - **[ISO-9001]** : http://www.iso.org/iso/fr/

1 – Une démarche qualité dans les unités de recherche

- **[ITIL]** : Information Technology Infrastructure Library
  - http://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
  - http://www.itilfrance.com/
- **[Deming]** : Roue de Deming
  - http://fr.wikipedia.org/wiki/PDCA
- **[ISO-20000-1]** : Technologies de l'information – Part1 – Gestion des services & Part 2 – Code of practice http://www.iso.org/
- **[ISO-27000]** : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences - http://www.iso.org/

2 – La gestion des configurations

Quelques systèmes logiciels permettant d'effectuer des administrations centralisées ou de gérer des configurations de parc de PC et un exemple de procédure d'ouverture de compte :

- **OCS Inventory** : Inventaire automatique de parc informatique et télédistribution

  Site Web http://www.ocsinventory-ng.org/
  Fiche Plume : http://www.projet-plume.org/fr/fiche/ocs-inventory-ng
- **cfengine :** administration automatisée de systèmes hétérogènes

Site Web : http://www.cfengine.org/
Fiche Plume : http://www.projet-plume.org/fiche/cfengine

- **NetDirector** : plateforme Web d'administration

  Site Web : http://www.netdirector.org/

- **Puppet :** permet d'automatiser un grand nombre de tâches d'administration : l'installation de logiciels, de services ou encore de modifier des fichiers.

  http://reductivelabs.com/trac/puppet

- **bcfg2** : Administration centralisée de serveurs

  http://trac.mcs.anl.gov/projects/bcfg2/

- **Quattor** :

  http://apps.sourceforge.net/mediawiki/quattor/index.php?title=Main_Page

- **Active Directory**

  http://fr.wikipedia.org/wiki/Active_Directory

  http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx

  http://www.adirectory.net/

- **Exemple de procédure d'ouverture de compte :**

  http://www.com.univ-mrs.fr/ssc/sic/spip.php?article43

3 – La gestion des niveaux de service

On trouvera ici des outils pour mesurer le niveau de service offert aux clients du S.I.

GLPI fournit des statistiques d'intervention qui permettent de mesurer le temps passé sur les demandes des utilisateurs

- GLPI : helpdesk associé à un outil de gestion
  - Site Web : http://www.glpi-project.org/
  - Fiche Plume : http://www.projet-plume.org/fiche/glpi

4 - La gestion de la continuité de service

On trouvera dans cette partie des logiciels permettant de surveiller les activités du réseau et des systèmes serveurs et donc d'analyser des causes de dysfonctionnement, d'y réagir promptement, améliorant ainsi la continuité des services.

- **Cacti** : logiciel de supervision réseau

  Site Web : http://www.cacti.net/

- **Ntop** : ntop est une sonde réseau qui permet de remonter et analyser le trafic réseau sous forme de graphe

  site web : http://www.ntop.org/overview.html

- Nagios : logiciel de supervision de réseaux et de systèmes (serveurs et postes de travail.)

Site Web : http://www.nagios.org/

- **Centreon** fournit une interface graphique pour permettre la consultation des informations issues de Nagios.

  Site Web : http://www.centreon.com/

- Webalizer : logiciel d'analyse des fichiers logs d'un serveur et de calcul des statistiques d'un site Web

  Site Web : http://www.webalizer.org/

Outre la surveillance réseau et système, la gestion de la continuité de service doit s'accompagner également d'un plan de continuité de service (actions d'urgence, sauvegardes des enregistrements vitaux, évaluation des dommages, plan de reprise...) et de systèmes logiciels permettant une reprise d'activité rapide

- **Heartbeat** : fournit une solution de haute disponibilité en mettant en place une redondance de serveurs en temps réel
  - http://www.linux-ha.org/
- **virtualisation** : Les systèmes de virtualisation permettent une souplesse dans l'administration et des réinstallations rapides; diminuant ainsi les durées d'indisponibilité
  - Journées josy sur la virtualisation : http://www.resinfo.cnrs.fr/spip.php?article3
  - **Xen** :
    - http://www.xen.org/
  - **Vserver**
    - http://linux-vserver.org/Welcome_to_Linux-VServer.org
  - **openVZ**:
    - http://wiki.openvz.org/Main_Page
  - **Proxmox (cluster de serveurs openVZ)**
    - http://pve.proxmox.com/wiki/Main_Page

5 - La gestion des interventions

On trouvera dans cette partie des logiciels permettant de formaliser un système de suivi de demandes entre les utilisateurs et le service informatique. Ce seront généralement des portails d'entrée qui permettront aux utilisateurs de poster leurs demandes d'assistance avec un certain degré d'urgence. Les demandes sont traitées par le service informatique. Des statistiques permettent de consulter les durées moyennes d'intervention, les durées d'attente avant prise en compte permettant ainsi d'afficher et d'améliorer le service rendu.

- **OTRS :** Open source Ticket Request System, distribué sous licence GPL fonctionne sur tout type de plate-forme.
  1. http://otrs.org/
- **GLPI** : helpdesk associé à un outil de gestion
  1. Site Web : http://www.glpi-project.org/

2. Fiche Plume : http://www.projet-plume.org/fiche/glpi

- **Request Tracker (RT)** : gestion de tickets d'incidents

1. Site Web : http://bestpractical.com/rt/

- **Helpdesk de ESUP-Portail** : c'est le système de suivi de demandes qu'on trouve dans ESUP-Portail qui est un Espace numérique de travail

1. http://www.esup-portail.org/display/ESUP/2008/08/22/esup-helpdesk+v3
2. http://www.esup-portail.org/display/PROJHELPDESK/esup-helpdesk+-+user+support+at+establishment-level

6 - La gestion des dysfonctionnements

Outils de remontées d'incidents :

- **Mantis** : Outil web de gestion des incidents : dépôt, validation, prise en compte, traitement et retour de signalement d'incident.
  - Site Web : http://www.mantisbt.org/
  - Fiche plume : http://www.projet-plume.org/fr/fiche/mantis
- **Bugzilla** : outil de gestion de bugs
  - http://www.bugzilla.org/about/
- **Gnats** : outil de gestion de bugs
  - Site Web : http://www.gnu.org/software/gnats/

Outils de remise en état initial d'un système permettant, par exemple de cloner des systèmes et de les restaurer pour remettre en service un système dans son état de base :

- **Mondo Rescue** : outil de « disaster recovery »
  - Site Web : http://www.mondorescue.org/
- **System Imager**
  - http://wiki.systemimager.org/index.php/Main_Page
- **PartImage**
  - http://www.partimage.org/Page_Principale
- **JeDDlaJ** :
  - http://la.firme.perso.esil.univmed.fr/website/rubrique.php3?id_rubrique=7

7 - La gestion des changements et de la mise en production

Des outils de type « main courante » :

- **elog** : site web permettant de déposer de l'information sous forme de messages texte horodatés de manière chronologique permet de tenir à jour un journal des modifications et interventions sur les différents éléments du SI (serveurs, config réseau, firewall, etc...).
  - https://midas.psi.ch/elog/#whatis

- **voila** : un tableau de bord synthétique des incidents et travaux
  - http://2007.jres.org/planning/paperfeed.html?pid=116

8 - La Documentation

Choisir un outil et un format d'édition efficace est communément accepté au sein de l'équipe d'ASR, pour rédiger la documentation technique propre au service.

- **[DocBook]** Le format **DocBook** est un langage de balisage conçu à l'origine pour la documentation technique informatique (matériel et logiciel). Il permet de produire une documentation de type papier : http://fr.wikipedia.org/wiki/DocBook
- **[Wiki] :** Les systèmes « Wikis» peuvent être de bons candidats pour rédiger et gérer une documentation. Les Wikis permettent la création et l'entretien collectif de sites Internet. On pourra notamment les utiliser pour déposer facilement de la documentation à jour au sein d'un service informatique.
- Une liste de quelques wikis les plus connus
  - http://www.framasoft.net/rubrique335.html
- Un comparatif de wikis :
  - http://www.wikimatrix.org/compare/DokuWiki+PmWiki+TikiWiki+TWiki
- **PMWiki** : http://www.pmwiki.org/wiki/PmWikiFr.PmWikiFr
- **MediaWiki** : http://www.mediawiki.org/wiki/MediaWiki/fr
  - **DokuWiki** : http://www.dokuwiki.org/
  - **TWiki** : http://www.twiki.net/

Les gestionnaires de contenu sur le Web (CMS) permettent également aux individus comme aux communautés d'utilisateurs de publier facilement, de gérer et d'organiser un vaste éventail de contenus sur un site web.

Les gestionnaires de contenu Web (CMS) :

- comparatif de serveurs de contenus :
  - http://2007.jres.org/planning/pdf/104.pdf
  - http://www.projet-plume.org/files/PLUME_Choix_Drupal.pdf
  - http://www.comparatif-cms.com/
- **Drupal** : http://drupalfr.org/
- **Spip** : http://www.spip.net/
- **joomla** : http://www.joomla.org/
- **WordPress** :http://fr.wordpress.org/

9 - Les bonnes pratiques dans la gestion de la sécurité des systèmes d'information

- **[EBIOS]** : méthode d'analyse de risques des systèmes d'information

- http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html

- **[PSSI CNRS]** :
  - http://www.sg.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/PSSI-V1.pdf
- [**A2IMP**] : Aide à l'acquisition d'informations sur machine piratée :
  - formation de l'UREC http://www.urec.cnrs.fr/article368.html
- [**A3IMP**] : Aide à l'Analyse des Actions Intentées sur une Machine Piratée
  - http://www.urec.cnrs.fr/article389.html
  - mise au rebut et recyclage des disques : *techniques d'effacement de disques avant mise au rebut*
  - *http://www.ipnl.in2p3.fr/perso/pugnere/effacement-disque-DP.pdf*
  - *http://www.ssi.gouv.fr/documentation/Guide_effaceur_V1.12du040517.pdf*
- **[ISO-27002]** : Techologie de l'information – Techniques de sécurité – Code de bonnes pratiques pour la gestion de la sécurité de l'information – http://www.iso.org/
- **[log cnrs] :** http://www.sg.cnrs.fr/FSD/gestrace.htm
- **[journaux systèmes] :** Journaux Systèmes : gestion des traces informatiques - problématique de centralisation des journaux et des traces informatiques :
  - http://www.jres.org/tuto/tuto7/index
  - http://www.jres.org/_media/tuto/tuto7/syslog-ng-tutojres.pdf
- Charte informatique du CNRS :
  - http://www.dsi.cnrs.fr/pre_BO/2007/03-07/tpg/charte-informatique.pdf
- sauvegardes de données:
  - http://www.resinfo.cnrs.fr/spip.php?article4
  - **backuppc** : http://backuppc.sourceforge.net/
  - **bacula** : http://www.bacula.org/fr/
  - **arkeia** : http://www.arkeia.fr/
  - **amanda** : http://www.amanda.org/
  - **time navigator** : http://fr.atempo.com/products/timeNavigator/default.asp
  - **netbackup** : http://www.symantec.com/fr/fr/business/netbackup
- Synchronisation des horloges systèmes
  - **ntp** : http://www.ntp.org/
- Contrôle d'accès aux systèmes – authentification
  - serveurs LDAP :
    - http://www.cru.fr/documentation/ldap/index
    - http://www.openldap.org/

- serveur Radius :
  - http://fr.wikipedia.org/wiki/Radius_(informatique)
  - http://freeradius.org/
- Active Directory
  - http://fr.wikipedia.org/wiki/Active_Directory
  - http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx
  - http://www.adirectory.net/

- mots de passe : nécessité de mot de passes solides
  - [CERTA-2005-INF-001] : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- contrôle d'accès au réseau
  - 802.1x :
    - http://fr.wikipedia.org/wiki/IEEE_802.1X
    - http://2003.jres.org/actes/paper.111.pdf
    - http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2005/sert-deprey/pres.htm
- cloisonnement des réseaux 802.1q
- architecture de réseau
  - http://www.urec.fr/IMG/pdf/secu.articles.archi.reseau.court.pdf
  - http://www.urec.cnrs.fr/IMG/pdf/articles.03.JRES03.archi.secu.slides.pdf
- contrôle de poste a distance , cyber-surveillance
  - VNC :http://www.realvnc.com/
  - TighVNC : http://www.tightvnc.com
- **[Chiffrement] :** Protection de transfert des données
  - http://www.sg.cnrs.fr/fsd/securite-systemes/documentations_pdf/journee_crssi/9-Chiffrement.pdf
  - http://igc.services.cnrs.fr
  - Quelques exemples d'outils de chiffrement des données sur les PC :
    - truecrypt : http://www.truecrypt.org/
    - Dm-Crypt, chiffrage de supports sous Linux : http://www.saout.de/misc/dm-crypt/
    - ZoneCentral : http://www.primx.eu/zonecentral.aspx

      Utilisation
  - SASL :
    - http://fr.wikipedia.org/wiki/Simple_Authentication_and_Security_Layer

    - http://asg.web.cmu.edu/sasl/
- Outils de métrologie et de surveillance réseau
  - **cacti** : http://www.cacti.net/
  - **Zabbix** : http://www.zabbix.com/
  - **openNMS** : http://www.opennms.org/wiki/Main_Page
  - **munin** :
    - http://munin.projects.linpro.no/ ;
    - http://fr.wikipedia.org/wiki/Munin_(Surveillance_système_et_réseau)
  - **ntop :** http://www.ntop.org/news.html
  - NetDisco :
    - http://netdisco.org/
    - http://en.wikipedia.org/wiki/Netdisco
  - **NfSen** : http://nfsen.sourceforge.net/
  - **smokeping** : http://oss.oetiker.ch/smokeping/

10 - Bonnes pratiques liées aux aspects juridiques du métier d'ASR – respect de la réglementation en vigueur

- Circulaire du 12 mars 1993 relative à la protection de la vie privée en matière de traitements automatisés.
- Loi n° 78-17 du 6 janvier 1978 informatique et libertés.
- Loi n° 83-634 du 13 juillet 1983 sur les droits et obligations des fonctionnaires.
- Recommandation n° 901 du 2 mars 1994 relative à la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.
- Décret n°81-550 du 12 mai 1981 relatif à la communication de documents et renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères.
- Guide n°400 SGDN/DISSI/SCSSI du 18 octobre 1991 relatif à l'installation des sites et systèmes traitant des informations sensibles ne relevant pas du secret de défense : protection contre les signaux parasites compromettants.
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
- Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (Article 30 et 31).
- Directive 485/SGDN/DCSSI/DR du 1er septembre 2000 sur la protection contre les signaux parasites compromettants.
- Recommandations nº600/SGDN/DISSI/SCSSI de mars 1993 relatives à la protection des informations sensibles ne relevant pas du secret de défense sur les postes de travail.

- La gestion des traces d'utilisation des moyens informatiques et des services réseaux au CNRS a été déclaré à la CNIL sous forme générique, pour l'ensemble des laboratoires sous tutelle CNRS et a fait l'objet d'une décision publiée le 11 octobre 2004 au bulletin officiel du CNRS (décision 04P014dsi.htm) http://www.dsi.cnrs.fr/bo/2004/12-04/4111-bo1204-dec04p014dsi.htm
- Articles relatifs à la réglementation en matière de sécurité, de protection du secret et de la confidentialité notamment ceux relatifs à la protection du patrimoine, au secret des correspondances écrites, aux sanctions pénales de la loi "informatique et libertés", pour les crimes et délits contre les personnes, les atteintes à la personne humaine et aux accès frauduleux à un système informatique et modifications frauduleuses.
- **[Legalis]** http://www.legalis.net : compte rendu des jurisprudences de différents tribunaux

11 - La gestion du temps

Vous trouverez dans cette partie trois références de livres utilisées dans le guide ainsi que quelques références internet liées au sujet :

- **[AdminSys]**: « Admin ' sys, Gérer son temps » de Thomas Limoncelli, traduit par Sébastien Blondeel, aux éditions Eyrolles :
  - http://www.editions-eyrolles.com/Livre/9782212119572/admin-sys
- **[GTD]** : « Getting Thing Done » est le titre d'un livre de David Allen publié en 2001, décrivant une méthode de gestion des priorités quotidiennes.
  - Divers articles à ce sujet sont présents sur http://avm.free.fr/ notamment la notion de Première Chose A Faire (PCAF) (http://avm.free.fr/spip.php?article26)
  - Plus connue sous l'acronyme GTD, sur wikipédia : http://fr.wikipedia.org/wiki/Getting_Things_Done
  - Un résumé de la méthode GTD par chapitre est donné sur http://gagnermavie.com/balade-a-travers-getting-things-done-chapitre-par-chapitre/
- Une comparaison des logiciels mettant en oeuvre la méthode GTD :
  - http://fr.wikipedia.org/wiki/Comparaison_de_logiciels_GTD
  - http://www.taskfreak.com/
- Plugins « GTD » : certains sont cités dans le document de comparaison ci-dessus. En particulier, le plugin GTD pour le Dokuwiki: http://www.dokuwiki.org/plugin:gtd
- **[résuméGTD]** : Un résumé de 7 pages du livre de David Allen : http://www.greyc.unicaen.fr/Members/Laurette%20Chardon/GbpFichePratiqueGestionduTempsDavidAllen.pdf ou https://www.greyc.fr/sites/default/files/GbpFichePratiqueGestionduTempsDavidAllen.pdf
- **[QuestionTemps]** : « Question de temps » de François Délivré, consultant en relations Humaines et Organisation, spécialisé dans le coaching des cadres dirigeants.
- Le résumé du livre de François Delivré : http://www.greyc.unicaen.fr/Members/Laurette%20Chardon/ResumeLivreQuestiondeTempsFrancoisDelivre ou https://www.greyc.fr/?q=user/14

12 - La communication de l'ASR avec ses partenaires

- **[GPLI], [RT], [Esup-Portail],[HelpDesk]** : voir les références données dans le chapitre 5 « Gestion des interventions ».

13 - Recommandations sur les compétences

Des liens liens utiles de sites des listes de diffusion

- [CRU] : https://listes.cru.fr/sympa/lists/informatique
- [CNRSlist] : http://listes.services.cnrs.fr/wws

Des liens liens utiles de réseaux de métiers

- [MRCT] : http://www.mrct.cnrs.fr/
- [RESINFO] http://www.resinfo.cnrs.fr/
- [UREC] : http://www.urec.cnrs.fr/
- [CRU] : http://www.cru.fr/

Des liens liens utiles de sites qui diffusent des tutoriaux ou (auto-)formations

- [CCM] : http://www.commentcamarche.net/
- [Zero] : http://www.siteduzero.com/
- [JRES] : http://www.jres.org/
- [TutoJRes] : http://www.jres.org/tuto/
- [Resinfo/Josy] : http://www.resinfo.org/spip.php?rubrique1
- [CUME] : http://cume.univ-angers.fr/index.php
- [Renater] : http://www.renater.fr/spip.php?rubrique45
- www.journaux.fr : liste par thème tous les magazines qui paraissent.
- [TDLP] : http://www.tdlp.org/ Linux documentation Project
- [LinuxFrance] : http://www.linux-france.org/ Linux-france
- [TutEns] : http://www.tuteurs.ens.fr/ Tutoriaux de l'ENS
- [MIT] : http://ocw.mit.edu/OcwWeb/web/home/home/ Open CourseWare du MIT (en anglais)

Liens vers des sites de veille technologique

- [ClubIc] : http://www.clubic.com/
- [ItEspresso] : http://www.itespresso.fr/
- [InterActu] : http://www.interactu.net/
- [Atelier] : http://www.atelier.fr/
- [Informaticien] : http://www.linformaticien.com/
- [UseNix] : http://www.usenix.org/ (en anglais)

Les nouvelles dispositions de la loi concernant la Formation Professionnelle

Extraits du décret :

Décret n° 2007-1470 du 15 octobre 2007 relatif
à la formation professionnelle tout au long de la vie des fonctionnaires de l'Etat
NOR : *BCFF0758784D*

Art. 1er. – L'objet de la formation professionnelle tout au long de la vie des fonctionnaires de l'Etat et des établissements publics de l'Etat est de les habiliter à exercer avec la meilleure efficacité les fonctions qui leur sont confiées durant l'ensemble de leur carrière, en vue de la satisfaction des besoins des usagers et du plein accomplissement des missions du service. Elle doit favoriser le développement professionnel de ces fonctionnaires, leur mobilité ainsi que la réalisation de leurs aspirations personnelles. Elle concourt à l'égalité effective d'accès aux différents grades et emplois, en particulier entre femmes et hommes, et facilite la progression des moins qualifiés.
La formation professionnelle tout au long de la vie comprend principalement les actions suivantes :

1° La formation professionnelle statutaire, destinée, conformément aux règles prévues dans les statuts particuliers, à conférer aux fonctionnaires accédant à un grade les connaissances théoriques et pratiques nécessaires à l'exercice de leurs fonctions et la connaissance de l'environnement dans lequel elles s'exercent ;

2° La formation continue, tendant à maintenir ou parfaire, compte tenu du contexte professionnel dans lequel ils exercent leurs fonctions, la compétence des fonctionnaires en vue d'assurer :
a) Leur adaptation immédiate au poste de travail ;
b) Leur adaptation à l'évolution prévisible des métiers ;
c) Le développement de leurs qualifications ou l'acquisition de nouvelles qualifications ;

3° La formation de préparation aux examens, concours administratifs et autres procédures de promotion interne ;

4° La réalisation de bilans de compétences permettant aux agents d'analyser leurs compétences, aptitudes et motivations en vue de définir un projet professionnel ;

5° La validation des acquis de leur expérience en vue de l'acquisition d'un diplôme, d'un titre à finalité professionnelle ou d'un certificat de qualification inscrit au répertoire national prévu par l'article L. 335-6 du code de l'éducation ;

6° L'approfondissement de leur formation en vue de satisfaire à des projets personnels et professionnels grâce au congé de formation professionnelle régi par le 6° de l'article 34 de la loi du 11 janvier 1984 susvisée.
Le contenu des formations prévues au 1° ci-dessus est fixé par arrêté conjoint du ministre intéressé et du ministre chargé de la fonction publique. Cet arrêté peut prévoir une modulation des obligations de formation en fonction des acquis de l'expérience professionnelle des agents.

Le CNRS et les Universités, par exemple, ont intégré ces dispositifs dans leur dossiers de suivi de carrière et en particulier la classification en 3 catégories des formations (paragraphe 2). Il faut aussi attirer l'attention sur les différentes possibilités de compléter son niveau initial de formation :

- la possibilité de réaliser des bilans de compétences (paragraphe 4)

- la procédure de VAE, Validation des Acquis d'Expérience (paragraphe 5)

Vous trouverez la déclinaison de la mise en œuvre de ce décret pour le CNRS aux URL suivants :

http://www.sg.cnrs.fr/drh/competences/form.htm

http://www.sg.cnrs.fr/drh/competences/documents/cadrage.pdf

14 - Outils Windows

Nous avons répertorié dans cette partie un certain nombre d'outils logiciels tournant sous *Windows* pouvant illustrer et être utilisés dans les différents chapitres de ce guide des bonnes pratiques.

Nous remercions à cet effet **D. Baba** *(Centre d'Immunologie de Marseille-Luminy, Unité Mixte de Recherche du CNRS, de l'Inserm et de l'Université de la Méditerranée)* pour son aide dans l'inventaire de ce type de produit « Microsoft »

- ***Administration des systèmes -*** *La gestion des configurations*

System Center ***(http://www.microsoft.com/france/serveur/system-center/default.mspx)*** est la gamme Microsoft d'outils et logiciels pour l'administration des S.I. Elle se veut aider les entreprises à simplifier leur administration informatique : exploitation plus facile, réduction des temps d'indisponibilité, automatisation des déploiements, et meilleure maîtrise du système d'information. On y trouve :

- SCOM 2007 (System Center Operation Manager), solution de supervision des environnements Windows offrant une collecte des événements et compteurs de performances, des fonctions de création de rapports et d'analyse de tendance. C'est une solution qui s'appuie sur des connaissances spécifiques par le biais de packs d'administration pour des environnements Microsoft et autres fournisseurs. Il se positionne comme un concurrent direct de IBM (Tivoli) ou de HP (Open View). La version SCOM 2007 R2 permet de superviser les systèmes UNIX et LINUX et les applications hébergées sur ces derniers.
- SCCM 2007 (System Center Configuration Manager), solution d'administration de parc informatique, changements et configuration, fournissant des fonctions d'inventaire (matériel et logiciels), ainsi que de télédistribution des applications et des mises à jour (sécurité et services pack), support à distance des postes et serveurs.
- SCDPM 2007 (System Center Data Protection Manager), application de sauvegarde à chaud et en continue des données avec possibilité de restauration par l'utilisateur et basé sur les technologies des clichés instantanées.
- SCVMM 2008 (System center Virtual machine manager), solution d'administration d'environnement virtualisé permettant une meilleure utilisation et optimisation des serveurs physiques. Supporte l'administration des serveurs VMware ESX.

- **Déploiement des postes de travail**

- WAIK (Windows Automated Installation Kit) est un Kit d'installation Windows automatisée qui permet de personnaliser et de déployer la famille des systèmes d'exploitation de Microsoft Windows Vista™. Windows AIK permet d'effectuer des installations Windows sans assistance, de capturer des images Windows avec ImageX et de créer des images

Windows PE qui est un mini-environnement de démarrage en mode commande basé sur Windows Vista. Téléchargement gratuit sur le site de Microsoft.

- WDS (Windows Deployment Services) permet de proposer aux postes de travail en réseau un ensemble d'images d'installation pour une migration ou mise à niveau. C'est un outil fournit avec le service pack 3 de Windows Serveur 2003 et intégré dans le WAIK. C'est une évolution de RIS (Remote Installation Services)
- Windows System Image manager, outil graphique pour créer et modifier les fichiers de réponse (unattended.xml), d'ajouter des composanst, etc…Il est fournit avec le WAIK.
- USMT 3.0 (User State Migration Tool) qui permet de sauvegarder les fichiers et paramètres de configuration du poste d'un utilisateur en vue d'une restauration après migration.
- Pour les phases d'un déploiement :
    - Application Compatibility Toolkit 5.0 pour la compatibilité logicielle
    - Windows Vista Hadware Assessment pour les configurations matérielles
- MDT 2008 (Microsoft Deployment Toolkit), permet l'automatisation de la gestion de cycle de vie du poste. Facilite l'automatisation des déploiements des postes de travail et des serveurs Windows. Il nécessite le WAIK.

• Continuité de service – Virtualisation

(http://technet.microsoft.com/fr-fr/virtualization/default.aspx)

- Hyper-V, technologie de virtualisation matérielle basée sur une approche de type hyperviseur. Disponible dans les éditions 64 bits des différentes versions de Windows serveur 2008. Egalement disponible en téléchargement. Il existe aussi une version qui peut être installé directement sur une machine vierge avec l'offre Microsoft Hyper-V server 2008.
- Virtual Server 2005 R2, virtualisation matérielle pour environnement Windows serveur 2003, utilisé surtout pour la consolidation et l'automatisation des tests (logiciels et développements), hébergement d'applications anciennes sur des matériels et OS récents et aussi pour la consolidation des serveurs. Produit gratuit
- Virtual PC 2007, solution de virtualisation de postes de travail permettant d'exécuter plusieurs systèmes d'exploitation en même temps sur le même ordinateur physique. Produit gratuit

• Sécurité et mobilité

- ISA serveur 2006 (Microsoft Internet Security and Acceleration) est une solution de pare-feu applicatif, de VPN (réseau privé virtuel), de proxy et cache web
- IAG 2007 (Intelligent Application Gateway) est un ensemble de technologies offrant la possibilité d'accéder de façon simple et sécurisé aux données et aux applications publiées à partir de nombreux appareils différents (PDA compris) et ceci depuis n'importe quel site relié à Internet

- **Gestion des correctifs de sécurités et de services pack**

- WSUS 3.0 (Windows server Update Services) est un produit qui permet de gérer de façon contrôlée les différentes mises à jour publiées sur le site de Microsoft Update (Correctifs, services packs, hotfix…). Produit téléchargeable sur le site de Microsoft.

- **Et enfin pour tous les utilisateurs avertis**

(http://technet.microsoft.com/fr-fr/sysinternals/default.aspx)

- La collection d'utilitaires SysInternals créée par Mark Russinovich et Bruce Cogswell et racheté depuis par Microsoft constitue une mine d'outils totalement indispensable pour des outils systèmes sous Windows : Utilitaires disques, Utilitaires réseau, utilitaires de ressources et de processus, Utilitaires de sécurité...