Guide de bonnes pratiques pour les Administrateurs Systèmes et Réseaux

Olivier Brand-Foissac, Laurette Chardon, Marie David, Maurice Libes, Gilles Requile, Alain Rivet

Le Livre

Guide de bonnes pratiques pour les Administrateurs Systèmes et Réseaux

Auteurs

Olivier Brand-Foissac, Laurette Chardon, Marie David, Maurice Libes, Gilles Requilé, Alain Rivet.

Ce site Web est la mise en ligne et l'édition numérique du livre « *Guide des Bonnes pratiques pour les Administrateurs Systèmes et Réseaux* » [ISBN 978-2-918701-07-1] paru en 2013 aux éditions MRCT du CNRS. Ce projet de guide est né à l'initiative de quelques ingénieurs ASR du CNRS réunis via le réseau métier **RESINFO**, et souhaitant mener une réflexion générale sur les différents contextes de travail de notre métier ASR.

Son objectif vise à déterminer les pratiques et les processus à mettre en place sur le terrain, pour une meilleure organisation du travail, afin d'améliorer la qualité et la fourniture de services, la sécurisation de nos serveurs et réseaux, la documentation de nos actions, la communication avec les utilisateurs, la prise en compte des évolutions technologiques, et i fine la lisibilité de nos activités d'ASR.

Vous trouverez tous les chapitres du livre dans le sommaire en haut a droite. En cliquant sur un chapitre, vous aurez le détail du sommaire du chapitre dans le menu à gauche.

Nous attendons de ce site Web une évolution et une mise à jour régulière du texte . Nous souhaitons la contribution des internautes et des lecteurs via le forum associé à chaque article. A la fin de chaque sous chapitre vous trouverez un lien *[forum: annoter le chapitre]* qui vous amènera au formulaire vous permettant de laisser toute annotation, texte, ou remarques constructives. Si vous laissez une annotation merci de bien indiquer à quel chapitre et sous chapitre il se réfère.

ISBN 978-2-918701-07-1

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 le cas pour les deux précédentes productions de RESINFO : SiLabo [1] et EcoInfo [2], 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. Dans ce guide le terme «ASR » fera référence, selon le contexte, soit à un individu isolé, soit à une équipe informatique, en charge de la maintenance des systèmes et réseaux des unités de recherche.

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.

Nous intégrons aussi dans les « Bonnes Pratiques » de l'ASR la prise en compte des conséquences sur l'environnement de l'utilisation de l'informatique. Un chapitre est consacré à ces aspects issus du groupe de travail ECOINFO de RESINFO, qui a déjà réalisé un gros travail sur ce thème. Nous reprenons 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 » répondent déjà à ces questions 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. Nous y ajoutons également des 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 dû 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 [7] et ISO 20000 [4] 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 qui serait nécessaire dans l'organisation de service. L'ASR reste généralement maître de proposer 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 : ISO 9001 [3], ISO 20000 [4], ISO 27001 [5]. 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 éléments de sortie ».

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 (SI) 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 [5] et est déclinée au CNRS sous le nom de PSSI [6]). Mais 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 (SI), la responsabilité civile, administrative ou pénale de la hiérarchie et des ASR pourrait dans certains cas, 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 sur ce sujet et transposées à notre métier.

On traitera donc 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

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 sont 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.

Aspects environnementaux

Enfin, il nous parait important de traiter cet aspect au travers du choix des matériels, des infrastructures et des comportements liés aux TIC qui ont des répercussions grandissantes dans plusieurs domaines environnementaux. Ces enjeux sont planétaires. Aussi quelques recommandations pratiques sont abordées afin d'en limiter l'impact.

Bien sur, nous serons attentifs à vos remarques et retours d'expériences sur les sujets abordés afin de mettre à jour ce guide en fonction des évolutions du métier.

Une démarche qualité dans les unités de recherche

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 SI (Systèmes d'Information) décrite par ITIL [7] (Information Technology Infrastructure Library) et plus récemment par la norme ISO 20000 [4].

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 matérialisée 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 de 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 entre autres :

- les rôles et responsabilités de la direction ;
- la gestion documentaire ;
- la gestion des compétences et de la formation ;
- la surveillance et les mesures.

La méthode PDCA (*Plan Do Check Act*), encore appelée roue de Deming [8], comporte quatre 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, réaliser, mesurer et analyser de façon progressive afin de travailler plus efficacement et, à terme, gagner du temps, de l'efficacité et augmenter le niveau de qualité des services rendus.

[forum : annoter le chapitre]

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 devaient être identifiables et mesurables dans l'ensemble des services informatiques de nos unités (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 recherche (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.

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.

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.

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 pour les besoins des utilisateurs.

Définir la continuité de service

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

Gérer les interventions

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

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.

Assurer les changements et les mises 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 propre, l'ISO 27001 qui sert de base à la mise en place des politiques de sécurité au sein des unités.

A travers ce guide, nous essayerons de préciser d'une part, ce qui nous paraît essentiel à mettre en place au sein d'un 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 unité de recherche.

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

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.

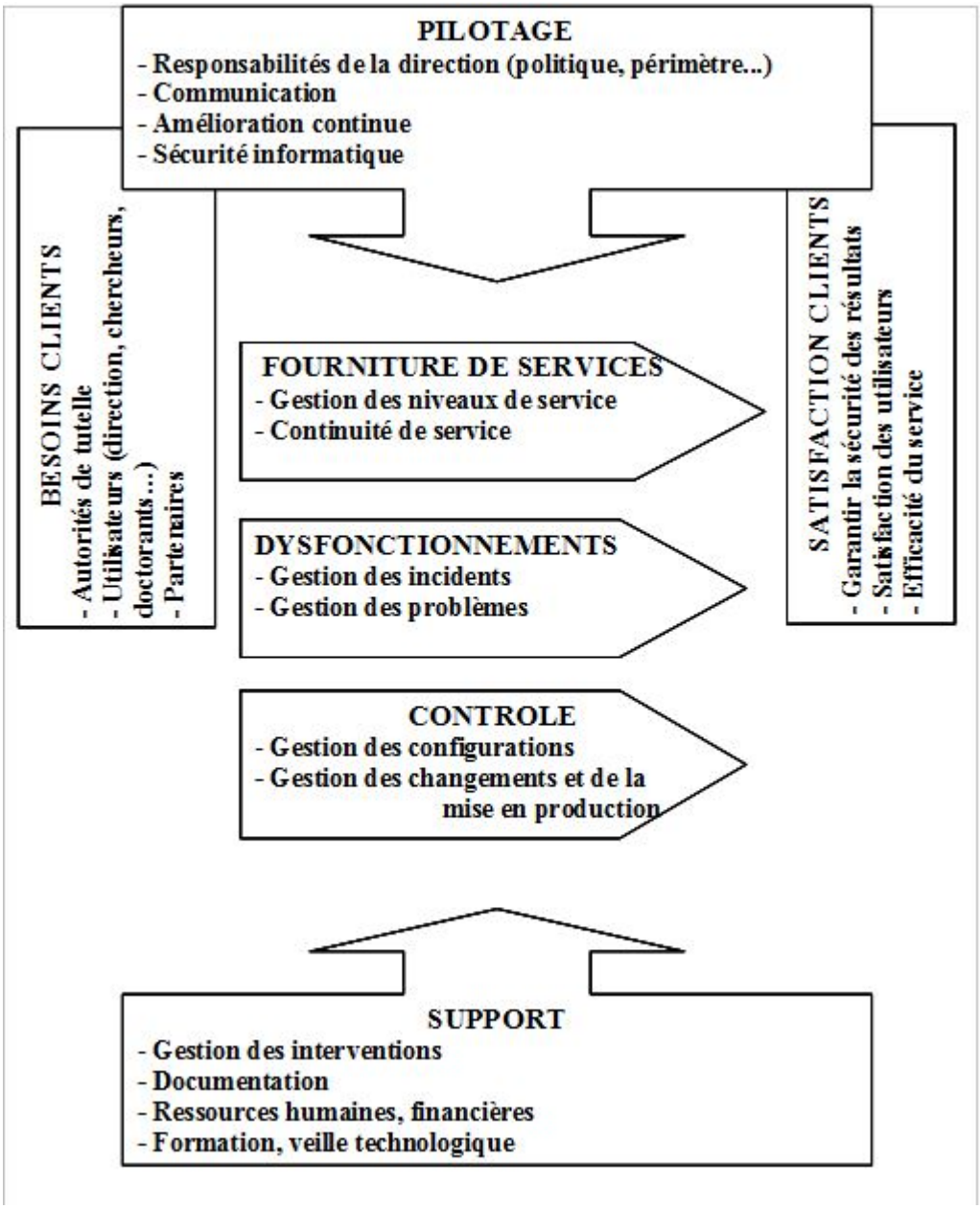


Figure 1 : Cartographie des processus dans un laboratoire de recherche

[forum : annoter le chapitre]

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 des services fournis dans un périmètre donné. L'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 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'unité : 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 service de noms, le serveur de messagerie, le réseau sans fil, par exemple, sont-ils pris en charge directement par le laboratoire ou par une autre structure de type CRI (Centre de Ressources Informatiques) ?
- 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 unités, et chaque unité 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'unité de recherche.

[forum : annoter le chapitre]

La gestion des configurations

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 nécessaires et préalables 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 ?
- A 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 la disposition des utilisateurs et comment ?
- etc.

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 doivent permettre 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 sont les incidences sur les autres éléments ?…) ;
- fournir des bases solides pour la gestion des dysfonctionnements ;
- comparer l'information stockée à l'infrastructure en place afin de corriger les différences.

[forum : annoter le chapitre]

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 semi-automatique avec des outils de gestion de parc.

On trouvera dans l'annexe 2 de ce guide un certain nombre de références vers des logiciels ou de la documentation qui peuvent servir et être utilisées par les ASR pour implémenter et mettre en place les différents volets requis dans la qualité de service.

[forum : annoter le chapitre]

La gestion des niveaux de service

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 ;
- de réaliser un suivi pour identifier et constater si les niveaux demandés ont été atteints et sinon 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, pour différents services supportés par les ASR dans nos unités (tels que, par exemple, la gestion du parc informatique, la maintenance des serveurs, la surveillance réseau, le déploiement d'application, les sauvegardes, l'archivage, les installations de PC pour le personnel de l'unité, l'assistance de premier niveau aux utilisateurs, etc.) d'associer des « niveaux de services ».

Par exemple :

Pour un service de « sauvegarde de données », le « niveau de service » pourrait être : *« les sauvegardes de données utilisateurs sont effectuées de manière quotidienne et conservées pendant 3 mois de manière glissante. Sur demande des utilisateurs, l'équipe Informatique procédera à des restaurations de données. Les données personnelles figurant dans le répertoire intitulé « personnel » présent dans tous les comptes informatiques ne seront pas sauvegardées ».*

Pour un service « d'installation de PC »… un « niveau de service » pourrait spécifier quelques éléments comme : « *Le service d'installation ne concerne que les PC achetés par le service informatique, pour les permanents du laboratoire, les installations se font aux heures ouvrables du lundi au vendredi, le PC est restitué à l'utilisateur sous 48 heures avec sa configuration réseau, un antivirus et les logiciels de bureautique de base sont installés. »*

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

- services métiers : disponibilité des moyens de calcul, de visualisation graphique, développements informatiques dédiés, support à la gestion financière et RH ;
- services infrastructures : gestion des serveurs, des sauvegardes, des impressions…
- services réseaux : gestion de la disponibilité du réseau, gestion des flux…
- services applicatifs : messagerie, web…
- …

La mise en place pratique d'un catalogue de service est présentée au chapitre 8 de cette partie.

L'ASR qui met en place une gestion de niveau de service doit s'assurer au préalable auprès de ses utilisateurs, des services utilisés et de leur usage. Ainsi, le cycle de la qualité de service passe par un engagement entre le service informatique et les utilisateurs de l'unité 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 nécessitent une authentification ;
- important : un service qui peut être interrompu brièvement. Exemple : messagerie, web, sauvegarde, serveurs de calcul, serveur anti-virus ;
- normal : un service qui peut être interrompu quelques jours. Exemple : un PC, une imprimante, un serveur de licences.

[forum : annoter le chapitre]

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 mêmes 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 ?
- …

[forum : annoter le chapitre]

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 lui est associée peuvent être remises en route dans les temps requis et convenus.

Depuis plusieurs années, l'interdépendance entre activités métiers et soutien informatique 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 7/7j et 24/24h du système d'information et des services informatiques.

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 ;
- …

[forum : annoter le chapitre]

La gestion des interventions

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 SI. 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, il est recommandé de 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.

[forum : annoter le chapitre]

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.

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, qu'elles soient matérielles ou humaines, s'effectuera à partir de cette fiche et une planification de l'intervention sera mise en place.

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.

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 SI. Il s'agit de minimiser leurs répercussions sur les niveaux de service mais également de prévenir leur réapparition.

La norme ISO 20000 distingue la notion d'incident de celle de problème. Un incident se décrit comme « 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-sous-jacente d'un ou de plusieurs incidents ». 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 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…).

[forum : annoter le chapitre]

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 SI 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 pu être utiles à la résolution du problème) ?
- Comment formaliser les solutions mises en place ?

Là encore, le service informatique devra définir les méthodes et outils qu'il convient d'utiliser pour mettre en place cette gestion des dysfonctionnements.

[forum : annoter le chapitre]

La gestion des changements et de la mise en production

Les changements au sein d'un service SI 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 à 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 SI 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, par exemple, la mise à jour système des serveurs du laboratoire ;
- avertir et informer les utilisateurs suffisamment tôt de l'interruption de service inhérente au changement de configuration ;
- accompagner les utilisateurs en cas de changement organisationnel qui pourrait impacter leur manière de travailler.

Avec un niveau de maturité supplémentaire dans l'organisation, l'ASR cherchera à apporter une vue la plus complète possible 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 ?

[forum : annoter le chapitre]

Le catalogue de services

Comme nous l'avons vu précédemment, les référentiels ITIL/ISO 20000 préconisent l'établissement d'un catalogue de services sans fournir concrètement de méthodologie de mise en application. L'objet de ce chapitre est donc de donner quelques pistes pour construire un catalogue de services qui ne soit pas un outil de plus à maintenir, mais un véritable moyen de gérer des services avec succès.

Utilité du catalogue de services

La gestion et l'organisation d'un service SI ne relèvent plus seulement de la gestion « de technologies ». Aujourd'hui, on demande de plus en plus au service informatique de l'unité d'assurer une meilleure visibilité de ses activités, de gérer les risques, d'argumenter ses dépenses et de savoir accompagner les évolutions en concertation avec les « métiers » de l'unité.

Un des moyens pour l'ASR d'atteindre ces objectifs est de disposer d'un catalogue de services qui peut devenir la base de la communication avec les métiers présents dans l'unité de recherche suivant les principes énoncés ci-dessous.

Le catalogue de services doit :

- être un moyen essentiel de communication et de coordination avec les métiers de l'unité. A ce titre, il permet de définir clairement et exhaustivement les services proposés, pour quelle population d'utilisateurs et les conditions de leur mise en œuvre. Dès lors, il convient de s'assurer que les services proposés sont bien en phase avec les besoins des utilisateurs ;
- ne pas être mis en place sans avoir fait un état des lieux des services existants ;
- être un outil accessible et de compréhension simple non seulement pour les utilisateurs, mais aussi pour les membres du SI. Il ne doit pas être ressenti comme un inventaire technique et incompréhensible ;
- permettre de disposer d'un langage commun avec les utilisateurs et la direction ;
- être tenu à jour et pouvoir évoluer, les besoins des utilisateurs n'étant pas figés dans le temps ;
- respecter au mieux les bonnes pratiques ITIL/ISO 20000, à savoir être documenté et évalué.

En préambule il est recommandé de prendre en compte les éléments suivants :

- Un utilisateur peut être vu comme un « client » à qui l'on propose un service dont il a besoin.
- Il faut commencer la démarche avec pragmatisme : recenser les services existants et démarrer sans vouloir être totalement exhaustif avec, par exemple, les services les plus utilisés, les plus demandés ou bien les plus critiques…
- Le catalogue de service doit permettre d'aboutir à de vrais engagements écrits avec ses utilisateurs au travers d'un contrat de service (*Service Level Agreement* ou SLA).
- Définir des niveaux de mesure (indicateurs, rapports réguliers…).

[forum : annoter le chapitre]

La démarche

Les cinq étapes suivantes sont fondamentales et nécessaires au bon fonctionnement de l'unité pour ne pas perdre de vue l'objectif principal qui est de se mettre en phase avec les besoins des utilisateurs :

- constituer un inventaire de l'existant : rassembler dans un premier temps les informations sur les services existants, en relation avec les utilisateurs, dans une phase d'identification des services (les

éléments renseignés peuvent prendre comme support la CMDB, si elle a été créée) ;

- compléter ces éléments par la mise en place d'interviews auprès des métiers de manière à identifier des besoins qui n'ont pas encore été traduits en services ;
- définir des critères qui permettront de prioriser les services afin de prendre les décisions de maintenir, remplacer, renouveler ou retirer ces services. Cela conduira à établir la liste des services à fournir ;
- fournir une vision synthétique des services pour lesquels le service SI s'engage vis à vis de ses clients dans le cadre de la formalisation d'un contrat de service ;
- communiquer les actions à entreprendre pour mettre en place les services à destination de l'ensemble des utilisateurs et proposer une vision « utilisateur » claire et ergonomique des services fournis (voir figure 3).

Ces différentes étapes devront être validées en relation avec la direction de l'unité, dans le cadre d'une commission informatique d'unité par exemple.

[forum : annoter le chapitre]

Identification des services

Cette étape essentielle va consister à réaliser un inventaire et une priorisation des services fournis ou à fournir par le service des systèmes d'information. Compte tenu des liens de dépendances entre services, il est indispensable de référencer les services métiers mais également les services supports ou techniques dont ils dépendent. En effet, on distingue, d'une part, les services directement perceptibles par les utilisateurs dans la pratique de leur métier (services métiers), et d'autre part les services proprement techniques, non directement perceptibles par les utilisateurs mais qui participent à leur soutien.

Exemple : l'installation d'une imprimante réseau est un service métier qui nécessite un service support qui est la gestion d'un serveur d'impression (non visible par le client).

La figure suivante permet de comprendre les relations qu'il faut établir entre services métiers et services supports.

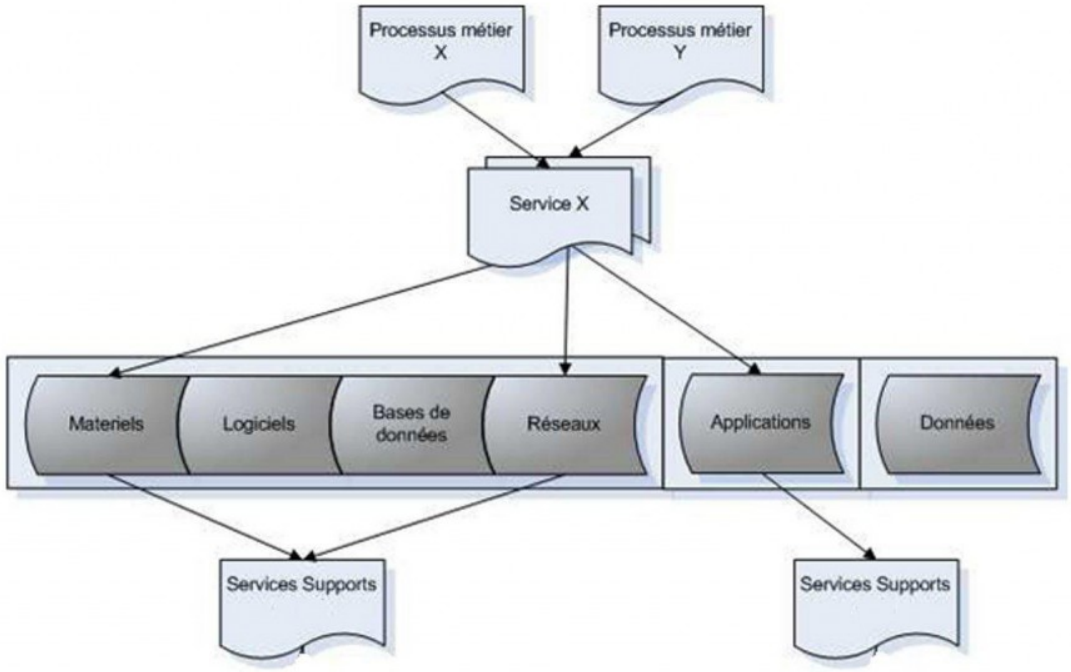


Figure 2 : Corrélation processus métier/support

Pour ce faire, il est intéressant de décrire les services à travers une matrice d'identification des services qui prendra en compte leur état, leur importance ainsi que leur composition (plusieurs niveaux ou imbrications de services).

Nous proposons un modèle d'identification des services à travers une feuille de tableur (tableau ci-après) qui comprend quatre parties distinctes, une partie inventaire, une partie processus et métier, une partie dépendances des services et une partie évaluation des niveaux de service.

INVENTAIRE

Identification des services		Visibilité	Etat du service		
1,3		Catalogue U	Utilisation	Gestion	Etat du service
19/11/2010		Oui; Non	Oui, Non	Interne, Externe	A l'Etude, Actif, Suspendu, Retiré
Nom Service	Description				
1 - Services Applicatifs					
Applicatifs Recherche (A décliner en N lignes)	....	Non			Actif
Applicatifs gestion administrative (A décliner en N lignes : financier, RH, Valorisation...)	....	Non			Actif
Applicatifs Bureautique		Oui	Oui	Interne	Actif
Autorité d'enregistrement CNRS Standard		Oui	Oui	Externe	Actif
Autorite d'enregistrement Terena			Non		
Disposer d'un espace Collaboratif	Diffuser, partager, échanger un ensemble d'informations (documents, plannings, PV de réunions...)	Oui	Oui	Interne	Actif
2 - Services Techniques					
2 - 1 Systèmes et Réseaux					
Gestion des OS		Non	Oui	Interne	Actif
Gestion des profils		Non	Oui	Interne	A l'étude
Accès à Internet		Non	Oui	Externe	Actif
Accès nomades		Non	Oui	Interne	Actif
Gestion des adresses mail		Non	Oui	Externe	Actif
2 - 2 Infrastructure					
Connectique		Non	Oui	Interne	Actif
Gestion des impressions		Non	Oui	Interne	Actif
Gestion des postes de travail		Non	Oui	Interne	Actif
Serveur GNP		Non	Oui	Interne	A l'étude
Serveur Web	Serveur Apache XXXX	Non	Oui	Interne	Actif
Serveur FTP		Non	Oui	Interne	Actif
Serveur InfoPC1		Non	Oui	Interne	Actif
Alimentation électrique		Non	Oui	Externe	Actif

PROCESSUS	DEPENDANCE	NIVEAU DE SERVICE			
Processus de l'entité		Niveau de service estimé			
Bilan	Bilan	Niveau de service estimé	Niveau de service ressenti	Nb utilisateurs impactés	Bilan
Niveau d'importance Maxi	Etat des dépendances	Opérationnel; Partiel; Inexistant		Un; Plusieurs; Tous	Niveau de service estimé
0	1				0,0
0	1				0,0
3	1				0,0
2	1				0,0
0	1				0,0
3	1	Partiel	Partiel	plusieurs	10,0
3	3				0,0
1	3				0,0
2	0				0,0
2	3				0,0
2	0				0,0
0	0	Opérationnel	Opérationnel	plusieurs	2,5
0	3	Partiel	Opérationnel	plusieurs	4,0
0	3	Inexistant	Partiel	plusieurs	8,0
0	0				0,0
0	0				0,0
0	0				0,0
0	0				0,0
0	0				0,0

Tableau 1 : Matrice d'identification de services

Voici brièvement, la description de cette matrice et des sections associées :

- la partie inventaire (colonne 1 à 6) permet de recenser les services et leurs caractéristiques de base, la visibilité éventuelle (dans le catalogue) du service et son état actuel (utilisation, type de gestion et état) ;

- la partie processus (colonne 7) permet d'associer les services décrits aux processus métier correspondants et de fournir un premier élément d'évaluation en fonction de leur criticité (importance pour le métier). Cette colonne, simplifiée pour l'exemple, peut être affinée et faire apparaître un découpage en processus de réalisation, de pilotage et de soutien de l'unité ;

- la partie dépendance (colonne 8) permet de décrire les interactions entre les services métiers et les services supports associés (services techniques qui viennent composer le service principal). Cette description prendra toute son importance lorsqu'il conviendra d'établir la fiche de description d'un service ;

- la partie niveau de service (colonne 9 à 12) permet d'évaluer les services décrits à partir des interviews conduits auprès de l'ensemble des parties prenantes (utilisateurs et service SI).

A partir de cette matrice, le service informatique en concertation avec la direction de l'unité et/ou une commission d'utilisateurs identifiera et validera les services retenus dont l'offre apparaîtra dans le catalogue de services.

[forum : annoter le chapitre]

Communiquer l'offre de services

L'étape suivante consiste à communiquer l'offre de service retenue auprès des utilisateurs. Cela peut être envisagé à deux niveaux, d'une part des fiches de description de chaque service et d'autre part une interface proposant une vue client du catalogue de services.

Fiche de description d'un service

Ce niveau de description décrit plus finement les services au travers de fiches unitaires de service qui visent à donner une vision synthétique de chaque service selon un modèle unique (tableau 2).

Il est possible d'élaborer la fiche à partir de la méthode QQOQCCP (Qui, Quoi, Où, Quand, Combien, Comment, Pourquoi) qui est une méthode de travail basée sur un questionnement systématique :

- Qui (quel collaborateur peut bénéficier de ce service) ;
- Quoi (qu'est-ce qu'est le service) ;

- Où (où s'adresser pour du support) ;
- Quand (délai de mise en œuvre et garantie de service) ;
- Combien (estimation du coût du service) ;
- Comment (moyen de demander ce service, et à qui) ;
- Pourquoi (liens utiles dans l'organisation).

La fiche d'identification de service fournit une série d'attributs descriptifs, parmi lesquels par exemple :

- l'objet de la prestation ;
- les moyens d'y accéder ;
- les garanties de la prestation (disponibilité du service, temps d'intervention…) ;
- les responsabilités ;
- le périmètre couvert ;
- l'appellation : le nom du service ;
- les objectifs du service, son utilité, les bénéfices apportés ;
- la disponibilité et la continuité de service ;
- les exceptions et les exclusions ;
- le public concerné ;
- les points de contact ;
- la durée, la pérennité, les plages de fonctionnement du service ;
- les dispositions éventuelles en matière de sécurité ;
- la mesure de la qualité fournie ;
- …

En ce qui concerne les garanties de la prestation, on peut être amené, selon le cas, à choisir entre une garantie en terme de disponibilité (en spécifiant une durée d'indisponibilité maximale), de temps d'intervention (durée maximale avant intervention après un incident), ou encore une garantie de temps de réponse. Le *Service Level Agreement* (SLA) représente ainsi l'engagement que le fournisseur de service prend vis à vis de l'utilisateur.

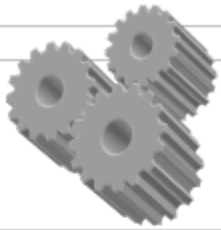
Titre Service	
	
Que pouvez-vous faire ?	
Qui peut bénéficier de ce service ?	
Comment disposer d'un espace collaboratif ?	**Délai de Mise en Œuvre**
Demande :	0 J
	Support
En cas de questions ou de problèmes, vous pouvez contacter le Support	A définir
Quelles sont les règles / restrictions à respecter ?	
Liens utiles	
Documentation utilisateur de l'UR	
Responsable de la fiche	**Date de dernière**
Prénom Nom Auteur	jj-mm-aaaa

Tableau 2 : Fiche d'identification de service

Vue client du catalogue de services

Pour améliorer la communication sur l'offre de services, le catalogue de services peut être mis à disposition de l'ensemble des utilisateurs à travers une interface web ergonomique donnant accès aux fiches de description des services décrites précédemment.

Voici ci-dessous un exemple avec le catalogue proposé par l'Université de Genève à travers le site web de la division informatique :

Figure 3 : Exemple de catalogue (https://catalogue-si.unige.ch/)

On pourra également s'inspirer du catalogue de l'Université de Strasbourg : (http://services-numeriques.unistra.fr/catalogue/service.html). ou celui de l'OSU Pytheas à Marseille https://sip.osupytheas.fr/?page_id=1735

En conclusion, la mise en place d'un catalogue de service ne se résume pas à développer un outil. Il ne faut pas perdre de vue que l'outil n'est qu'un moyen et non une fin.

Le catalogue de services conduit à structurer et organiser les services offerts. Vis-à-vis des utilisateurs et des partenaires, il devient une interface essentielle car il formalise et rend compte de l'activité du service. A ce double titre, il est réellement intégré dans une démarche qualité. Il doit être ainsi réévalué périodiquement dans le cadre du processus d'amélioration continue (modèle PDCA).

[forum : annoter le chapitre]

La documentation

Nous avons souligné précédemment l'importance de la formalisation des méthodes de travail au sein d'un SI pour améliorer la qualité dans la fourniture de services informatiques. 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 SI, 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 SI. 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 (*Content Management System* ou CMS) [9] ou encore un *wiki* [10].

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 SI.

On distinguera deux grandes classes de documentation que l'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.

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. Cette documentation est très importante par le fait qu'elle peut rendre les utilisateurs autonomes en limitant l'appel systématique aux ASR.

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

- un catalogue de service qui affiche les services fournis ainsi que les accords sur les modalités et niveaux de service offerts par l'équipe informatique, les usages tolérés, les règles de conduite ;

- 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 ou un catalogue de service ;

- 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 en *ssh*, comment paramétrer son PC pour accéder au service d'authentification des Universités (*Eduroam*...) ;

- les règlements (souvent rassemblés dans le règlement intérieur de l'unité 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.

[forum : annoter le chapitre]

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, *Access List* de routeurs mises en place, noms et adresses internet 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 l'installation de tel ou tel logiciel, ou bien les causes et les résolutions d'incidents qui sont survenues dans le SI, 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 installé et paramétré : comment est configuré *samba*, comment est assurée la redondance du serveur de mail au moyen d'*heartbeat* ou autres... ;
- 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.

[forum : annoter le chapitre]

Comment réaliser ces documentations ?

Le but de ces documentations est qu'elles soient facilement accessibles, modifiables, partageables, correctement structurées, classées et en accès protégé.

L'ASR aura le choix du mode d'édition de ces documentations : documentation papier, fichier au format *DocBook* [11], site web ou w*iki*, etc.

Les dépôts documentaires de type *wiki* peuvent à cet effet procurer certains 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.

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 système majeur qui empêcherait la consultation en ligne.

La mission d'un organisme de recherche consiste à produire et valoriser des connaissances, aussi, l'information qui est générée et transmise s'avère de nos jours un patrimoine essentiel de nos unités qu'il convient de préserver. Comme le rappelait un Fonctionnaire de Sécurité de Défense du CNRS : « Les entreprises, les laboratoires de recherche, les administrations regorgent d'informations dont la compromission peut nuire gravement aux intérêts de l'établissement, quand ce n'est pas aux intérêts nationaux (technologies innovantes, recherches duales, contrats industriels, données personnelles, données médicales… la liste est longue) ».

Les enjeux de la sécurité des systèmes d'information

La sécurité de l'information est définie comme la « protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ». Elle devient aujourd'hui une des problématiques majeures de nos unités.

Forts de ce constat, nous devons envisager la finalité de « protection du patrimoine scientifique » à travers des enjeux principaux :

- garantir la disponibilité de l'outil de travail pour l'ensemble des personnels de la structure ;
- garantir la confidentialité des informations, qu'elles soient professionnelles ou personnelles ;
- garantir l'intégrité des informations et des personnes ;
- assurer la protection des données sensibles de la structure (données scientifiques et techniques, données de gestion administrative, données individuelles) ;
- assurer la protection juridique (risques administratifs, risques pénaux, perte d'image de marque).

La mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) à travers la norme ISO 27001 [5] apparaît comme une réponse aux besoins de protection des données de nos unités de recherche dans un contexte de démarche qualité (PDCA).

[forum : annoter le chapitre]

La construction du Système de Management de la Sécurité de l'Information (SMSI)

L'apport des normes ISO 2700x

La norme ISO 27001 a été publiée en 2005 et est disponible en français depuis juillet 2007. Elle constitue le référentiel pour la mise en œuvre d'un système de management de la sécurité de l'information. La mise en place d'un SMSI est une démarche transverse qui concerne tous les métiers et activités d'une structure de recherche. Elle doit aider à la réalisation des objectifs communs dans un souci de gestion de la confidentialité, de l'intégrité et de la disponibilité du patrimoine informationnel.

La norme ISO 27001 [5]s'appuie sur une série de documents associés :

- ISO 27002 détaille les 133 mesures de sécurité listées dans l'annexe de l'ISO 27001 et regroupées en 39 objectifs de sécurité, eux-mêmes classés en 11 domaines (politique de sécurité, sécurité du personnel, contrôle des accès…). Les objectifs de sécurité présentent un but à atteindre et les mesures de sécurité présentent les activités permettant d'y parvenir et expliquent les actions à mettre en œuvre pour implémenter ces mesures ;

- ISO 27004 explique comment mettre en œuvre des indicateurs pour mesurer la pertinence du SMSI ;

- ISO 27005 est un socle important de la mise en œuvre du SMSI, puisqu'il décrit l'appréciation des risques de la sécurité de l'information de l'ISO 27001.

[forum : annoter le chapitre]

Les différentes étapes de mise en place du SMSI

On l'a vu précédemment, le SMSI s'appuie sur un modèle d'amélioration continue (appelé PDCA ou « Roue de Deming » [8]) qui conduit dans un premier temps à fixer les objectifs du SMSI (*Plan*), à le déployer (*Do*), puis à vérifier les écarts éventuels entre ce qui a été défini et ce qui est mis en œuvre (*Check*), enfin à mettre en place les actions qui permettront de corriger ces écarts et améliorer le SMSI (*Act*).

Etape de planification « Plan »

Dans cette étape on se doit de définir le périmètre que l'on va gérer dans le SMSI : périmètre géographique mais surtout périmètre en termes d'activités de la structure de recherche (périmètre d'activité de recherche, d'enseignement, d'administration, périmètre par métier, etc.). Il faut bien s'attacher à prendre en compte également les interfaces avec les fournisseurs, partenaires externes…

Il faut choisir et mettre en place une méthode d'analyse de risques pour déterminer, évaluer et couvrir les principaux risques qui peuvent peser sur le SI de l'unité . Cette méthode prendra en compte les étapes suivantes :

- l'étude du contexte, la définition des seuils d'acceptation des risques ;
- la cartographie et la classification des actifs primordiaux et actifs de soutiens ;
- l'identification des menaces, l'analyse des vulnérabilités ;
- l'identification des situations de risques, la classification des risques ;
- le traitement des risques retenus : la liste des risques couverts et non-couverts et le choix des solutions pour couvrir les risques ;
- la définition des coûts, bénéfices, impacts des solutions retenues ;
- l'acceptation des risques résiduels par la direction.

Pour terminer l'analyse on doit déterminer quelles sont les mesures de sécurité que l'on doit prendre pour couvrir les risques. On verra que ces mesures sont recensées dans un document particulier exigé par la norme appelée « déclaration d'applicabilité » (DdA).

Pour une structure déjà en place cette étape passe nécessairement, par un état des lieux de l'existant et surtout par un recensement des mesures qui sont déjà en place (on part en effet rarement de rien) : inventaire des documents existants et des mesures déjà appliquées. A quel degré sont-elles déjà conformes avec le SMSI ? Existe-t-il déjà une appréciation des risques ?

Certains écueils sont à éviter lors de cette phase importante de l'analyse des risques, notamment il est nécessaire de prendre en compte les ressources (financières, matérielles, humaines…) réellement disponibles, les freins psychologiques et surtout les réels enjeux

métiers de la recherche.

Etape du déploiement « Do »

Après l'analyse de risques, il est nécessaire de déployer les mesures de sécurité décidées dans le plan de traitement des risques et retenues dans la DdA.

Il est également nécessaire de former et sensibiliser les personnels. En effet rien ne sert de mettre en place des mesures si les personnels n'en sont pas informés et ne sont pas sensibilisés aux bonnes pratiques de sécurité. De même il ne sert à rien d'installer des outils de sécurité si ceux qui doivent les utiliser ne sont pas formés.

Enfin, il faut gérer le risque au quotidien par la détection et la réaction rapide aux incidents et la génération d'indicateurs au fil de l'eau.

Étape de vérification « Check »

C'est une étape fondamentale dans un SMSI puisqu'il s'agit de vérifier :

- qu'il n'existe pas d'écarts majeurs entre ce que le SMSI définit et ce qui est mis en œuvre en pratique ;
- que les mesures de sécurité qui couvrent les risques les plus critiques sont adaptées, efficaces et suffisantes.

Les indicateurs et les outils permettant ces contrôles sont multiples. Il peut s'agir par exemple de la liste des incidents de sécurité, des indicateurs de contrôle, des tableaux de bord sécurité, des rapports d'audits internes, des enregistrements de non-conformité produits par le SMSI, des revues de direction, etc.

Il faut garder à l'esprit, lors de cette étape, que les contrôles ne sont pas mis en place pour mesurer l'efficacité « théorique » du SMSI (celle décrite sur le papier), mais surtout l'efficacité des mesures appliquées.

La phase *Check* du SMSI doit permettre l'exécution des procédures de surveillance et de réexamen afin de détecter rapidement les erreurs à traiter et identifier rapidement les failles de sécurité et les incidents de sécurité.

Cette phase doit permettre de s'adapter aux changements :

- réexaminer à intervalles planifiés l'appréciation du risque ;
- s'adapter aux changements d'organisation, de techniques, d'objectifs de l'unité, de menaces, d'efficacité des mesures de sécurité, de réglementation…

Pour cela, il conviendra de mettre en place un suivi des améliorations possibles qui seront prises en compte lors de la phase *Act* suivante (entreprendre des actions correctives ou préventives).

Étape d'ajustement « Act »

Il s'agit de définir, lors de cette étape, les actions qui permettront de réaliser les corrections et les améliorations du SMSI, mises en évidence par les indicateurs lors de l'étape précédente, mais également de prendre en compte tout changement éventuel intervenu entre temps dans le système d'information (mise en place par exemple d'un nouveau matériel stratégique…) :

- un changement de périmètre (technique, organisationnel ou fonctionnel) ayant un impact sur le périmètre du SMSI ;
- de nouveaux risques (nouvelles menaces apparues, nouvelles vulnérabilités).

Les actions résultantes seront classées en trois catégories : actions correctives (sur incident ou écart constaté), actions préventives (sur une anomalie potentielle), actions d'amélioration (amélioration de la performance du processus existant).

Organiser la mise en place pratique d'un SMSI dans les unités de recherche

Etant donné l'importance des processus à mettre en place, il est à notre sens irréaliste à ce jour de vouloir mettre en place un véritable SMSI complet de type ISO 27001 dans nos unités de recherche. Nous allons donc, dans ces lignes, nous limiter à un SMSI « allégé » propice pour parvenir à la mise en place d'une Politique de Sécurité opérationnelle du Système d'Information dans l'unité (PSSI). En complément de l'aspect didactique du guide qui présente globalement le SMSI, pour conserver un aspect pratique nous mettrons l'accent sur la gestion du risque.

Engagement de la direction et lancement du SMSI

Tout d'abord, un SMSI est un acte de direction. Celui-ci doit donc émaner officiellement

de la direction d'une unité. Il est illusoire de vouloir initier un SMSI sur la seule base du bénévolat ou des compétences techniques ou organisationnelles d'un agent bien formé et volontaire.

Il convient que la direction définisse des dispositions générales claires en accord avec ses objectifs et qu'elle démontre son soutien et son engagement vis-à-vis de la sécurité de l'information en mettant en place et en maintenant une organisation propre à construire une politique de sécurité de l'information pour tout l'organisme.

Il est donc nécessaire que le Directeur d'Unité (D.U.) lance officiellement le démarrage d'une démarche SMSI et qu'il désigne un comité de pilotage. Ce groupe peut être composé de plusieurs membres représentatifs des différentes fonctions de l'unité par exemple : un membre de la direction (directeur adjoint par exemple), un personnel administratif, un personnel technique, des chercheurs et enseignants. Il va de soi qu'un représentant du service informatique, s'il existe, devrait y être présent.

Ce lancement peut passer par un document officiel et formel comme une autorisation de lancement de la part du directeur d'unité. Ce document rappellera qu'il est nécessaire de respecter :

- les dispositions législatives et réglementaires, les directives de niveau supérieur (ministérielles et interministérielles) ;
- les différentes recommandations des politiques SSI des tutelles.

Le document indiquera qu'il convient de lancer une analyse de risques permettant d'identifier ce qui doit être protégé dans le périmètre concerné, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité afin que l'unité se donne une politique de sécurité conforme à ses intérêts.

Étude du contexte et de l'environnement

Cette étape est importante car c'est sur elle que reposera le processus de gestion du risque. L'étude comprend trois parties successives :

- la présentation de l'unité : il faut d'abord présenter l'unité afin d'identifier ce qui est important pour son fonctionnement telles que sa structure, ses missions, son organisation et sa stratégie ;

- les contraintes : on s'attachera à analyser et à rappeler les différentes contraintes qui affectent l'organisation parmi lesquelles, par exemple, des contraintes réglementaires, budgétaires, calendaires (dates d'examens, de remise de rapports scientifiques…), politiques, fonctionnelles, ou encore culturelles (par exemple envisager le fait que certaines expérimentations scientifiques doivent pouvoir se faire en dehors des heures ouvrables…) ;

- le choix du périmètre : il doit servir à définir le périmètre géographique à sécuriser (les locaux, bâtiments…), mais également les actifs de l'unité (matériels, logiciels, personnels…) qui supportent l'information à sécuriser. Dans la norme ISO 27000, ces « actifs » sont de deux types :

- les actifs « primordiaux » représentent les fonctions essentielles de l'unité comme par exemple « acquérir des données scientifiques, rédiger des publications, assurer les commandes de l'unité… », ainsi que les informations nécessaires à l'accomplissement de la mission (résultats de recherches, contrats de partenariat, informations nominatives…) ;

- les actifs « de soutien » représentent l'ensemble des matériels (PC, serveurs, réseau…), logiciels (logiciels métiers scientifiques et administratifs), mais aussi les locaux ou encore les personnels (chercheurs, enseignants, administration…) qui supportent et manipulent les informations à sécuriser.

Ce périmètre peut être volontairement restreint lors de la mise en place du SMSI, il sera progressivement étendu lors des révisions ultérieures dans un processus d'amélioration de la qualité (démarche PDCA).

Cette étude préliminaire du contexte débouche sur une étude de l'appréciation des risques et plus globalement de gestion des risques que nous allons détailler.

[forum : annoter le chapitre]

La gestion du risque

Dans la mise en place du SMSI, la « gestion des risques » est un processus essentiel qui permet de définir des exigences de sécurité qui seront traduites en objectifs de sécurité qui à leur tour vont impliquer la mise en place de mesures de sécurité adaptées. Dans ce cadre,

plusieurs référentiels utiles à la mise en œuvre d'un tel système sont disponibles.

La gestion du risque comporte deux grandes étapes : l'appréciation des risques et le traitement des risques.

Un risque est la conjonction de trois facteurs :

- une vulnérabilité d'un actif de soutien (matériel, logiciel, personnel humain…) : par exemple une salle serveur peut ne pas être climatisée ou ne pas posséder un contrôle d'accès ;
- la probabilité qu'un évènement menaçant (incendie, pirate…) exploite cette vulnérabilité : par exemple en l'absence de climatisation de la salle serveurs, l'augmentation de température engendrée par les machines hébergées peut occasionner une surchauffe, et le déclenchement d'un incendie ;
- un impact et des conséquences plus ou moins importantes résultant de la réalisation de cette menace : perte des données scientifiques et administratives de l'unité. En l'absence de sauvegardes, l'activité de l'unité est paralysée pour plusieurs semaines.

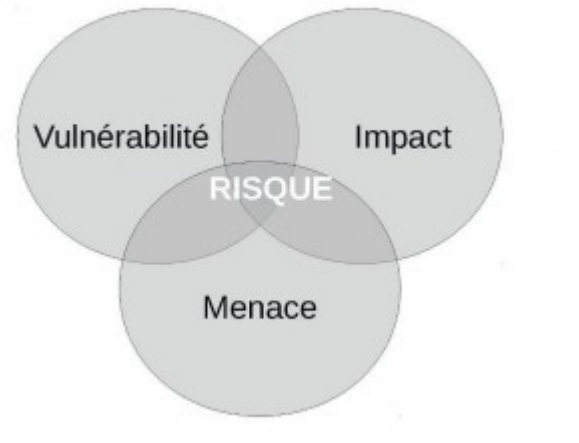


Figure 4 : Illustration des composants d'un risque en SSI

Un risque est qualifié en fonction de l'impact qu'il peut avoir et de sa probabilité ou vraisemblance d'occurrence. Pour analyser les risques on va passer par deux étapes :

- détermination / identification des risques : on détermine quels sont les principaux

risques qui pèsent sur les éléments du SI ;

- valorisation des risques : on calcule une valeur (un poids) pour chacun des risques en fonction de la probabilité d'occurrence d'une menace, de la facilité d'exploitation d'une vulnérabilité, et des impacts qui en découlent.

On sera donc amené à classer et à prioriser les risques selon la valeur calculée et d'en proposer un traitement.

Au final, le traitement des risques consistera à décider quelles mesures prendre ou pas pour diminuer ou éliminer le risque, en s'appuyant sur un référentiel de bonnes pratiques (le volet ISO 27002) associant objectifs et mesures de sécurité.

Pour chaque risque identifié, le traitement selon la norme sera ramené à quatre actions possibles :

- refuser le risque (*i.e.* supprimer au moins un des trois critères de définition d'un risque, voire supprimer la fonction générant le risque) ;
- réduire le risque (modifier les critères de vulnérabilité, la probabilité de réalisation des menaces, l'impact, jusqu'à un niveau de risque acceptable appelé risque résiduel) ;
- transférer le risque (transférer la fonction qui génère le risque à une autre unité) ;
- accepter le risque (par exemple si celui-ci est faible ou trop couteux à éliminer…).

[forum : annoter le chapitre]

Appréciation du risque

L'appréciation des risques consiste, d'une part, à les identifier, et d'autre part à les évaluer c'est-à-dire les exprimer avec une valeur qui caractérise leur importance.

Définition des échelles de valeurs

Avant de commencer l'analyse de risques proprement dite, il est important de se doter de diverses échelles de notation et d'évaluation qui seront nécessaires pour « quantifier » les risques et leur affecter une priorité (abaque).

Nous allons détailler successivement ces différentes échelles de valeur :

1. une échelle de valeur des actifs (quels sont les actifs les plus importants ?) ;
2. une échelle de vraisemblance des menaces (quelles sont les menaces les plus probables ou les plus vraisemblables ?) ;
3. une échelle de facilité d'exploitation des vulnérabilités ;
4. une échelle d'importance des impacts ;
5. un tableau de classification des risques.

[forum : annoter le chapitre]

Les niveaux de valorisation des actifs

Le CNRS, par exemple, propose dans le cadre de ses formations sur la mise en place de la Politique de Sécurité des Systèmes d'Information (PSSI) [6] au sein des unités de recherche, les cinq valeurs suivantes pour la valorisation des actifs :

- valeur négligeable (coefficient 0) : si cet actif vient à manquer, les effets ne sont pas décelables ;
- valeur faible (coefficient 1) : si cet actif vient à manquer, les effets affectent essentiellement des éléments de confort ;
- valeur significative (coefficient 2) : si cet actif vient à manquer, les effets affaiblissent la performance ;
- valeur élevée (coefficient 3) : si cet actif vient à manquer toute l'unité est impactée ;
- valeur critique (coefficient 4) : si cet actif vient à manquer les missions essentielles de l'organisme sont mises en danger.

[forum : annoter le chapitre]

Échelle d'estimation des menaces

On évalue les menaces à partir de leur vraisemblance (ou leur probabilité d'occurrence) dans le contexte de l'unité. La vraisemblance d'une menace se mesure à partir de scénarios d'attaques : types de menaces environnementales ou humaines, existence d'attaquants, motivations d'attaque…

On trouvera une liste de 42 méthodes d'attaques possibles dans le volet ISO 27005 ou dans la méthode Ebios [12] et [13] (comme par exemple, l'incendie, le vol, les écoutes réseau, etc.).

L'estimation des menaces peut ainsi s'évaluer sur une échelle à trois niveaux selon la vraisemblance ou probabilité d'occurrence : probabilité faible, moyenne et forte, notées de 1 à 3.

[forum : annoter le chapitre]

Échelle d'estimation des vulnérabilités (facilité d'exploitation)

Il convient dans un premier temps de répertorier les vulnérabilités présentes sur les actifs de soutien, puis pour chacune d'elles, de déterminer leurs facilités d'exploitation en tenant compte des mesures de protection existantes.

Pour chaque actif de soutien de l'unité on va estimer la facilité d'exploitation de leurs vulnérabilités :

- vulnérabilité très facile à exploiter (coefficient 1) : par exemple une salle serveur peut avoir comme vulnérabilité d'avoir une climatisation défectueuse ou de capacité insuffisante. L'augmentation de température qui peut s'ensuivre peut être un facteur de déclenchement d'incendie. Le déclenchement d'un incendie qu'il soit d'ordre environnemental ou intentionnel ne nécessite aucune compétence et est de ce fait facile à exploiter ;

- vulnérabilité moyenne (coefficient 2) : par exemple, le système de messagerie peut laisser passer certains documents comportant des virus. Les PC de l'unité ne sont pas tous équipés d'antivirus. Cette vulnérabilité est moyennement facile à exploiter du fait que certaines mesures antivirales sont déjà prises dans l'unité, et que l'unité a une architecture réseau sécurisée (réseau segmenté en vlan et filtres entre les réseaux) qui minimise les diffusions virales ;

- vulnérabilité difficile à exploiter (coefficient 3) : par exemple, le logiciel de gestion du service de noms (DNS) souffre d'un bogue de sécurité permettant de corrompre le cache des adresses IP de l'internet. Cette vulnérabilité potentiellement très dangereuse et spectaculaire nécessite toutefois des compétences très importantes relevant de spécialistes pour être exploitée.

[forum : annoter le chapitre]

Établissement des critères d'impact

Il faut répondre à la question : à partir de quel niveau juge-t-on qu'un impact est assez important pour que le risque soit pris en compte ? Les niveaux d'impact peuvent être confondus avec les niveaux de valorisation d'un actif définis précédemment, à sa perte ou sa dégradation.

Cinq niveaux dans les critères d'impacts / conséquences :

- négligeables : les effets ne sont pas décelables (coefficient 0) ;
- faibles : les effets affectent essentiellement des éléments de confort (coefficient 1) ;
- significatifs : les effets affaiblissent la performance de l'unité (coefficient 2) ;
- élevés : toute l'unité est impactée (coefficient 3) ;
- critiques : les effets mettent en danger les missions essentielles de l'organisme (coefficient 4).

Par exemple :

- impact important (coefficient 3 à 4) : l'incendie de la salle serveur en raison de la défaillance d'une climatisation peut avoir un impact catastrophique pendant plusieurs semaines pour la poursuite des activités de l'unité ;
- impact moyen (coefficient 2 à 3) : en l'absence de dispositif de sauvegarde de données, la perte ou le vol d'un PC peut compromettre une expérimentation et les activités d'une équipe sans toutefois paralyser l'unité entière ;

- impact faible (coefficient 1) : dans des conditions de sécurité déjà présentes (présence d'antivirus sur la majorité des PC de l'unité, sensibilisation permanente des utilisateurs et filtrage sur les serveurs de messagerie) la contamination de quelques PC dans l'unité fera perdre tout au plus quelques heures à l'utilisateur et au service informatique.

Attention toutefois aux impacts « faibles » lorsque les événements sont multipliés à plus grande l'échelle : par exemple un virus qui impacte quelques PC dans une unité peut devenir un vrai fléau à l'échelle nationale lorsque plusieurs centaines d'unités sont concernées.

A titre indicatif, le volet ISO 27005 (2008) propose comme critères de mesure de l'impact de considérer les points suivants :

- niveau de classification des informations impactées ;
- réduction d'opérations, internes ou avec partenaires externes (empêche la réalisation complète d'une opération) ;
- perturbations de plans, dépassement de *dead line* (notamment si des actions sont en cours avec des partenaires extérieurs, grand projets, etc.) ;
- dommages à la réputation (des équipes de recherche, de l'unité, des tutelles).

[forum : annoter le chapitre]

Exemple d'évaluation de l'importance des risques

Avec ses 3 facteurs constitutifs (vulnérabilité, menace et impact), le risque peut donc être évalué à travers différentes formules (la norme n'impose pas de formule précise) reliant ces trois facteurs : Risque = fonction (impact, menace, vulnérabilité).

A partir de ces critères, on peut combiner ces trois facteurs par une formule qui permettra de donner une valeur à différents niveaux de risques.

L'abaque ci-après, proposé par le CNRS, équivaut à une formule :

Risque = (Menace + vulnérabilité + Impact) – 2

Dans ce tableau, le risque est ainsi maximal (valeur de 8) dans le cas d'un impact critique (4) avec de fortes probabilités de menaces (haute) et une vulnérabilité élevée (facile).

Vraisemblance de la menace		Faible (1)			Moyenne (2)			Forte (3)		
Exploitation de la vulnérabilité		Basse (1)	Moy. (2)	Elevée (3)	Basse (1)	Moy. (2)	Elevée (3)	Basse (1)	Moy. (2)	Elevée (3)
Impact (Valeur d'actif)	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tableau 3 : Abaque d'appréciation du risque

(Source : cours dispensés par la cellule sécurité du CNRS lors de formations en 2008 et 2009)

En fonction des coefficients que l'étude a permis d'affecter aux menaces et aux actifs de soutien, et donc du niveau de risque calculé, le tableau suivant permet de caractériser cinq zones d'évaluation du risque et plusieurs manières de le traiter.

0		Risques nuls (0)	Risques acceptables
1	2	Risques négligeables (1-2)	Risques acceptables
3	4	Risques significatifs (3-4)	Risques à traiter au cas par cas
5	6	Risques graves (5-6)	Risques à traiter systématiquement
7	8	Risques vitaux (7-8)	Refus du risque tant qu'il n'a pas été traité

Tableau 4 : Zones d'évaluation du risque

L'étape consiste, en fonction des objectifs internes de l'unité, à définir des seuils d'acceptation du risque, cela conduit par voie de conséquence à définir les risques qui seront traités en priorité.

[forum : annoter le chapitre]

Audit de sécurité auprès des experts métiers

Après que les abaques et les divers critères d'appréciation du risque aient été définis, il

convient que le groupe de travail chargé de la SSI de l'unité mette en place une série d'entretiens auprès des experts métiers (chercheurs, administratifs, enseignants…) présents dans l'unité.

L'objectif de ces entretiens est de faire s'exprimer les différents experts métiers de l'unité et de comprendre leur besoins de sécurité en termes de disponibilité, confidentialité de leurs données et processus métiers.

Ces divers entretiens permettront d'analyser les besoins et de valoriser les actifs primordiaux et les actifs de soutien de manière globale et homogène au sein de l'unité.

Bien entendu, les écueils à comprendre et éviter sont souvent que chaque expert métier, non spécialiste de la SSI, peut avoir une vision partielle ou erronée de sa situation individuelle en terme de besoins de sécurité. La tendance étant alors soit de sous-estimer le risque (« je n'ai pas de données sensibles », « je n'ai rien à cacher »), soit de le surestimer (« je ne peux supporter un arrêt de la messagerie plus d'une heure »). Le rôle de l'expert SSI au vu de son expérience peut être alors de dialoguer, faire comprendre les enjeux et trouver un compromis acceptable qui resitue les besoins dans le contexte général et permette de mieux cerner les objectifs de sécurité.

[forum : annoter le chapitre]

Traitement des risques

Traiter le risque c'est donc se référer aux procédures, codes de conduite, règles de sécurité, normes, standards et dispositifs techniques, ayant pour objectif la protection du système d'information de l'organisme.

Le traitement du risque va consister à décider si le risque est accepté, refusé, transféré ou réduit. La réduction du risque va entraîner la sélection de mesures de sécurité. Dans le cas où l'on veut réduire le risque, le choix de ces mesures passe par l'identification des objectifs de sécurité (que veut-on protéger et pourquoi ?) et le choix des mesures de sécurité adaptées.

Exemple de risque refusé :

- Risque de perte de données scientifiques issues d'expérimentation et de missions scientifiques. Ces données sous-tendent l'activité de publication du laboratoire et sa renommée scientifique :

- vulnérabilité : climatisation trop ancienne et insuffisante dans la salle serveurs et absence de moyens de sauvegarde, plusieurs interruptions de la climatisation en été ;

- menace : élévations fréquentes de la température en salle serveurs, menace d'incendie ou de dégradation des disques supportant les données scientifiques ;

- Objectif de sécurité : on veut obtenir une disponibilité, une confidentialité et une intégrité élevée des données scientifiques acquises en missions ou d'expérimentation. On ne peut supporter la perte de données. Ces données doivent être sauvegardées sur un média externe et restituées en cas de problème.

Exemple de risque transféré :

- Réception importante et fréquente de virus et de spams par la messagerie électronique. Le service informatique du laboratoire en sous-effectif investit trop de temps dans la maintenance du serveur de messagerie de l'unité. Dans la conjoncture actuelle, il n'y a pas de valeur ajoutée à ce que l'unité conserve un serveur de messagerie en interne. La direction décide de « transférer » le risque et demande à ce que le service de messagerie soit pris en charge par l'organisme hébergeur.

Le traitement du risque dépend en effet des objectifs de sécurité que l'unité s'est fixée. Les objectifs de sécurité expriment la volonté de couvrir les risques jugés inacceptables sans préjuger des solutions pour y parvenir. Ils découlent logiquement de l'appréciation des risques.

Un exemple d'expression d'objectifs de sécurité concernant la disponibilité des données pourrait être : « Eviter les dommages dans les locaux comportant les données essentielles de l'unité ». Nous trouvons l'expression d'un tel objectif dans l'annexe A.9.1 de l'ISO 27001 :

- [A.9.1] Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur les informations de l'organisme.

A.9 Sécurité physique et environnementale
A.9.1 Zones sécurisées
Objectif: Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur les informations de l'organisme.

Figure 5 : Premier extrait de l'annexe de l'ISO 27001

L'objectif de disponibilité des données de l'unité est également exprimé dans le maintien des moyens de traitement de l'information. L'annexe A.10.5 est un objectif nécessaire pour mettre en place des mesures de sauvegarde des informations :

- [A.10.5] Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.

A.10.5 Sauvegarde		
Objectif: Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.		
A.10.5.1	Sauvegarde des informations	*Mesure* Des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

Figure 6 : Second extrait de l'annexe de l'ISO 27001

Les mesures de sécurité qui découlent de ces objectifs donnés en exemple sont :

- les zones sécurisées seront protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel habilité est admis ;
- des mesures de protection physique contre les dommages causés par les incendies doivent être conçues et appliquées ;
- des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

L'annexe de la norme ISO 27001:2005 représente les mesures de sécurité génériques qui couvrent les risques. Ces mesures sont détaillées dans le document ISO 27002.

Pour déterminer les mesures de sécurité appropriées à chacun des risques identifiés, on

pourra utiliser l'annexe A de l'ISO 27001. Ce document qui associe les objectifs de sécurité et les mesures associées comporte 133 mesures structurées en 11 chapitres, couvrant l'essentiel des domaines de la sécurité.

Ce catalogue de mesures s'avère très utile et permet d'être sûr de ne pas oublier une mesure importante même si toute latitude est autorisée pour mettre en place des mesures de sécurité non mentionnées. La norme ISO 27002 [5] est en fait un véritable « guide de bonnes pratiques » en matière de SMSI et présente en détail les 133 mesures précédentes accompagnées de recommandations concrètes d'experts en sécurité.

Une fois le traitement du risque mis en œuvre, il conviendra de déterminer les risques résiduels qui subsistent une fois les mesures de sécurité appliquées de façon à les prendre en compte dans la réactualisation de l'analyse des risques.

[forum : annoter le chapitre]

Déclaration d'applicabilité

La dernière étape de la gestion des risques, dans sa phase de « traitement » consiste à dresser un tableau récapitulatif reprenant l'ensemble des 133 mesures de l'Annexe A de l'ISO 27001.

L'ensemble de ces 133 mesures sera consigné dans un document intitulé Déclaration d'Applicabilité (DdA ou SoA pour *Statement of Applicability* en anglais) qui contient pour chaque objectif de sécurité, les mesures de sécurité retenues, les raisons de leur sélection mais également les mesures de sécurité non retenues et les raisons de leur mise à l'écart. Pour la réalisation de ce document, aucune mesure n'est à priori obligatoire même si les exigences de la norme ISO 27001 et les obligations règlementaires ou statutaires rendent plusieurs mesures incontournables.

La DdA est le document fondamental demandé par la norme auquel il est nécessaire d'aboutir pour mettre en place un SMSI. Il représente la synthèse des mesures de sécurité nécessaires pour sécuriser l'unité. Il s'appuie sur l'ISO 27002 qui est un guide de bonnes pratiques en matière de mesures de sécurité. Pour chacune des 133 mesures de sécurité apportées par la norme ISO 27002, la DdA permet d'indiquer les raisons de la sélection des mesures ou de leur rejet.

Ainsi les mesures de sécurité qui peuvent être sélectionnées seront le fait des exigences de sécurité suivantes :

- imposées par la norme ISO 27001 ;
- imposées par les contraintes légales et réglementaires, par exemple, présentes dans la PSSI de la tutelle ;
- imposées par le contexte ou les bonnes pratiques : certaines mesures sont évidentes ;
- issues de l'appréciation des risques ;
- déjà mises en place.

[forum : annoter le chapitre]

Bénéfice de la démarche SMSI

Au vu des éléments précédents, le projet de mise en place d'un SMSI permet de mobiliser l'ensemble des acteurs de la structure de recherche autour d'un projet commun. Chaque acteur, depuis l'utilisateur final, jusqu'à la direction de la structure, en passant par l'équipe informatique, prend sa part de responsabilité dans la sécurité de l'information.

Cette implication ne s'obtient concrètement que par l'engagement fort de la direction qui doit s'affirmer de manière claire et visible. En retour, la mise en place d'un SMSI apporte à la direction de l'unité des règles de bonne conduite, l'aidant à gérer ses objectifs et à répondre à des questions simples mais fondamentales (où se trouvent les informations sensibles de ma structure ? Sont-elles bien conservées ? Sont-elles bien protégées eu égard aux contextes et enjeux scientifiques ?…).

Le deuxième domaine d'intérêt concerne le fait d'impliquer l'ensemble des métiers de la structure dans la gestion des risques qui pèsent sur le patrimoine informationnel. On l'aura compris, la sécurité n'est pas qu'une affaire de technique, mais aussi et surtout de politique, d'organisation et de comportement.

Par cette démarche et des pratiques qui en découlent, l'ASR trouve sa légitimité dans la bonne prise en compte des mesures de sécurité à déployer et à accompagner. Il sera renforcé dans son rôle de « force de proposition » pour conduire ce projet et n'aura sans doute plus le sentiment d'être isolé dans son unité en mettant en œuvre, de par ses décisions personnelles, des mesures de sécurité le plus souvent techniques qui ne couvrent qu'une partie des risques potentiels.

Enfin, faire connaître auprès des tiers et de ses partenaires sa nouvelle gouvernance concernant la protection de son patrimoine et le respect des contraintes réglementaires pourra apporter plus de confiance et de professionnalisme dans les relations réciproques.

[forum : annoter le chapitre]

5. Exemples de mesures de sécurité courantes

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

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 carte ou code).

Pour se protéger des menaces d'ordre environnemental, il convient également de mettre en œuvre des dispositifs de détection et d'alerte de température élevée, d'incendie ou d'inondations ou d'autres formes de sinistres provoqués soit accidentellement soit par malveillance.

[forum : annoter le chapitre]

Sécurité du matériel et du câblage

On protégera les matériels sensibles (routeurs, serveurs…) des pertes d'alimentation électrique par un système de secours bien dimensionné, 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 réseaux transportant des données doivent être protégés contre toute possibilité d'interception de l'information, ou de dommage. Les câbles ou concentrateurs réseaux doivent être hors de portée immédiate et donc protégés dans des gaines ou des armoires de répartition.

[forum : annoter le chapitre]

Mise au rebut ou recyclage

Les matériels, les informations ou les logiciels ne devraient pas pouvoir être sortis des unités sans autorisation préalable au vu d'une procédure formelle. En cas de mise au rebut ou 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 [14].

Les supports qui ne servent plus doivent être mis au rebut de façon sûre. Il n'est pas conseillé pour des raisons environnementales de même que pour des raisons de sécurité du SI de se débarrasser des PC et des supports amovibles dans des bennes non spécialisées, ni sans avoir au préalable correctement effacé les supports (magnétiques, etc.).

[forum : annoter le chapitre]

Procédures de sécurité informatique liées à l'exploitation

5.4.1 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 et CERTA [15], 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.

5.4.2 Sauvegarde des informations

La sauvegarde des informations est un processus essentiel permettant de garantir la disponibilité des données 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 et ces informations de sauvegarde doivent être communiquées aux utilisateurs. Une sauvegarde régulière des données des utilisateurs ainsi qu'un processus de restauration, testés au préalable, doivent être mis en place. Les droits d'accès à ces sauvegardes doivent faire l'objet d'une attention particulière.

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 doivent aussi être testées régulièrement conformément à la politique de sauvegarde convenue.

5.4.3 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 sur l'intranet du CNRS [16].

Il est important de protéger les serveurs qui conservent les informations journalisées contre des accès non autorisés ou des actes de malveillance 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 [17].

5.4.4 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 unités de recherche soient synchronisées à l'aide d'une source de temps précise et préalablement

définie.

5.4.5 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 la 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 unités. La segmentation du réseau de l'unité en réseaux logiques virtuels (VLAN) est donc une bonne mesure à prendre pour séparer des flux réseau de différentes entités administratives (le réseau des chercheurs, le réseau des étudiants, le réseau de secrétariats, le réseau des serveurs…). Cette différenciation 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 SI doit être protégé des tentatives d'accès illicites provenant de l'extérieur comme de l'intérieur de nos unités. Des mesures de 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 unités. Les flux d'entrée, et de sortie, du réseau doivent également être protégés par un ensemble de filtres
(ACL dans le jargon) qui permettent d'interdire des accès réseau vers des ressources

ou des services non contrôlés.

5.4.6 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 TLS, IMAPS, SSTPS, 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 [18] et le site de l'ANSSI [19][20].

Il est important pour les ASR de connaître le fonctionnement des certificats et leur mise en œuvre. Dans le cas du CNRS, par exemple, l'ASR se rapprochera des Délégations Régionales (DR) pour connaître les modalités d'obtention et d'utilisation des certificats électroniques afin de fournir des certificats aux utilisateurs de son unité ainsi qu'aux serveurs administrés qui en nécessitent. Pour les cas de multi-tutelles, ces certificats peuvent aussi être sollicités auprès des autres tutelles.

5.4.7 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 informatiques des utilisateurs destinée à accorder ou 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 unique 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 à partir d'un processus formel contrôlé de manière à empêcher l'utilisation de mots de passes trop faibles (utiliser des 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 système d'information des unités.

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

5.4.8 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.

5.4.9 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 système d'information implique une surveillance de l'utilisation du réseau et des serveurs tout en respectant la réglementation en vigueur (cf. les aspects juridiques du métier d'ASR dans ce guide). 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.

[forum : annoter le chapitre]

Sauvegarde et archivage

Quelle que soit l'unité de recherche concernée, il y a production et utilisation d'informations sous forme de données numériques. Une des fonctions de l'ASR est de proposer des dispositifs qui permettent d'assurer une préservation de ces données en cas de perte accidentelle ou autre. La duplication de ces données par stockage redondant sur des supports différents de ceux de l'équipement utilisé (poste de travail fixe, mobile, serveur, …) est un des principes de base. Elle nécessite la mise en place de techniques et de procédures de stockage et de restauration spécifiques au type de donnée concernée.

Ces recommandations sont notamment issues de la norme NF-Z-42-013 (2001) [20] qui fournit des spécifications relatives à la conception et l'exploitation de systèmes en vue d'assurer la conservation et l'intégrité des documents stockés, dans le domaine de l'archivage électronique. Y sont abordées diverses recommandations d'organisation et de bonnes pratiques concernant la gestion des supports WORM (*Write Once Read Many*) mais qui peuvent aisément être transposées à d'autres types de sauvegarde et d'archivage.

Il convient donc de distinguer clairement les deux finalités :

- la sauvegarde, quelle que soit sa forme et son usage, est destinée à mémoriser des données évolutives de manière à en conserver la persistance et pouvoir les restituer en cas d'accident. On peut couramment considérer que les données stockées sont régulièrement modifiées (écrites, effacées) ;

- l'archivage, en revanche, consiste à rendre accessible en lecture des données immuables (archives de documents administratifs, données de mesures expérimentales, résultats de simulations coûteuses à produire, etc.), bien que leur classification puisse évoluer dans le temps (métadonnées associées).

La durée de rétention, les modes d'accès et souvent les volumes, sont fondamentalement différents, ce qui suppose que des supports, des nommages, des lieux d'hébergement adaptés et une gestion des risques devraient leur être appliqués (notamment en cas de risque de perte accidentelle et en cas de sinistre). Le critère le plus important qui distingue ces deux aspects sera la durée du cycle de vie.

La quantité d'informations traitées dans nos unités a une nette tendance à augmenter. Tant pour les sauvegardes que pour l'archivage, certaines techniques comme la déduplication, pourront, à fonctionnalité constante, réduire le volume des données et les

coûts d'infrastructure.

La norme propose par exemple des méthodes d'identification des supports ainsi que des processus d'enregistrement de leur chaînage. A intervalle régulier, des copies de sécurité doivent être effectuées (fréquence et nombre dépendant de la criticité des données, de la durée de vie des supports dans l'environnement de conservation…) et stockées loin des originaux. D'une manière générale, les sauvegardes et archivages doivent être systématiquement vérifiés et régulièrement testés. Il peut arriver que des supports deviennent illisibles, dans ce cas les systèmes d'écriture/lecture doivent être vérifiés et une copie de sécurité régénérée et identifiée.

Cependant, l'archivage pose des problèmes particuliers propres à la longue durée de rétention des données. Typiquement, on peut trouver actuellement des supports garantis au moins 30 ans (magnéto-optiques notamment). En revanche, les matériels et logiciels permettant d'exploiter ces supports survivent rarement au-delà de 10 ans. Il en va de même de la possibilité d'exploiter les formats des informations stockées sur ces supports. C'est un paradoxe de l'archivage électronique : conserver des données pendant de longues durées en s'appuyant sur des technologies rapidement obsolètes. Quelques règles simples de bonnes pratiques nous permettront de minimiser les risques liés à ce paradoxe tout en respectant disponibilité, intégrité et confidentialité des données.

[forum : annoter le chapitre]

Imposer des standards indépendants des applications et des environnements informatiques

Ne pas perdre de vue que la lecture, le décodage ou la transcription doivent rester pérennes durant toute la durée de conservation. Privilégier les formats ouverts (soit libres, soit dont les caractéristiques sont publiées) est un gage de pérennité (XML, HTML, PDF/A sont les plus cités en ce qui concerne les documents texte). L'interopérabilité consistant à pouvoir transférer les données d'un système à un autre devrait s'imposer à tout système d'archivage.

L'obsolescence rapide de la plupart des supports impose (en particulier pour les données conservées plus de 5 ans) d'envisager dès l'origine la migration en tenant compte des formats logiques mais aussi du temps nécessaire et de l'indisponibilité éventuelle occasionnée.

[forum : annoter le chapitre]

Respecter la législation

Les données peuvent faire l'objet de restrictions d'accès, voire de déclarations (données personnelles, etc.). L'archivage est autant concerné que le stockage, d'une manière générale, par ces aspects juridiques. Certains documents notamment administratifs doivent être probants. Il conviendra d'assurer l'intégrité de ces documents tout au long de leur durée de conservation (Code Civil Art.1316-1 [21]).

[forum : annoter le chapitre]

Pérenniser les données descriptives

L'augmentation du nombre et du volume de données va de pair avec les données descriptives (métadonnées) permettant de les situer (origine, dates, etc.), de les retrouver (classification, indexation, etc.), éventuellement d'en mémoriser les accès (données protégées ou sensibles) et de s'assurer de leur intégrité (signature, empreinte, chiffrement…).

La sauvegarde des systèmes de gestion des données descriptives fait partie intégrante de l'archivage des données elles-mêmes. Ainsi, une base de données d'index ou de mots-clés permettant la recherche de documents dans un thésaurus d'archive est à sauvegarder, simplement pour maintenir opérationnel l'accès aux documents, voire parce que la reconstitution d'un tel index peut s'avérer un processus long et complexe.

[forum : annoter le chapitre]

Analyse de risques et politique d'archivage

Conserver les données sur le long terme, les retrouver et les restituer avec fidélité dans un format intelligible tout en sécurisant leur accès constituent les objectifs de l'archivage électronique. Une analyse de risques portant sur les données d'archivage ainsi que sur les moyens d'y accéder permettra de définir une politique de sauvegarde propre à l'unité.

La politique d'archivage doit conduire à :

- définir les objectifs du système (services rendus) ;
- préciser l'ensemble des intervenants et leurs responsabilités ;
- définir les fonctionnalités (versement, stockage, administration) ;

- préserver l’environnement sécuritaire associé en lien avec la politique de sécurité du système d’information.

Elle permet de transformer les exigences en différents niveaux de service eux-mêmes traduits en architecture technique et en processus.

Ce chapitre rédigé par le groupe de travail GBP a été réalisé à partir de diverses formations et conférences juridiques données par Maître BARBRY [22].

Schéma du droit de la Sécurité des Systèmes d'Information

La présente note vise à actualiser le schéma de synthèse des ***textes applicables au droit des systèmes d'information*** élaboré en juin 2015 à la lumière des évolutions législatives et réglementaires françaises et européennes intervenue en 2016 et 2017

- SchemaDroitSSI2015NotesActualisation

Le schéma ci dessous donne une vision synoptique des textes impactant le travail des ASR. Il fait suite à un travail de mise a jour régulier que nous avons entrepris avec Me E. Barbry (cabinet Racine, spécialiste du droit en SSI) car le droit en SSI a connu de fortes évolutions ces dernières années

L'idée de ce schéma est de donner un panorama du droit de la SSI et de l'état des textes réglementaires qui affectent les interventions informatiques des ASR dans nos unités CNRS

Schéma juridique du droit en SSI (mise à jour 2018)

Dans cette vidéo Me Barbry explique les principales évolutions de la SSI en 2018 : GBP-schema-SSI-Barbry

http://gbp.resinfo.org/wp-content/uploads/2018/08/GBP-schema-SSI-Barbry.mp4

Référentiel légal du métier d'ASR

Il n'existe pas de référentiel légal concernant le métier d'ASR. Autrement dit, le terme d'« Administrateur Systèmes et Réseaux » n'apparaît dans aucune loi, décret ou texte réglementaire, contrairement au Correspondant Informatique et Liberté (CIL), dont la fonction et les responsabilités sont bien définies dans un cadre légal.

Deux points sont tout de même à noter. Tout d'abord, l'arrêté du 18 juillet 2010 relatif au secret défense [23] parle de l'administrateur dans sa fonction « sécurité » : on commence donc à lui attribuer un statut juridique dans un cadre particulier. Ensuite, le second point concerne deux guides pratiques de la CNIL [24a] et [24b]. Ce ne sont pas des textes réglementaires mais ils sont une conséquence de la loi « Informatique et Libertés » du 6 janvier 1978. Le premier guide à destination des employeurs et des salariés définit dans sa

fiche pratique n°7 la mission de l'administrateur réseau. Le second guide relatif à la sécurité des données personnelles parle, entre autres, de la sécurité des postes de travail et de celle des serveurs et des applications (fiches n°4 et n°11).

La jurisprudence nous apporte également quelques précisions sur le régime juridique des ASR. L'une précise [25] que la fonction des ASR nécessite de pouvoir faire des investigations, certes, mais indique que les résultats de celles-ci n'ont pas à être divulgués. Un devoir déontologique de réserve s'impose.

La seconde [26] confirme le licenciement de l'ASR d'une association qui a téléchargé 24h/24 et 7j/7 environ 6 Go d'images, de sons et de vidéos considérant qu'il avait abusé de ses droits privilégiés au système informatique.

L'ASR, de par sa fonction, a des accès privilégiés aux ressources et systèmes de son unité. Il doit donc être particulièrement vigilant dans la mise en œuvre des moyens qu'il utilise. L'environnement juridique actuel nous permet de retenir quelques bonnes pratiques énoncées ci-après.

[forum : annoter le chapitre]

Ne pas ignorer le droit.

Avec ses accès privilégiés sur les réseaux et systèmes, l'ASR peut accéder plus facilement à des données relevant de la vie privée résiduelle des utilisateurs, à leurs données personnelles, à des données relevant de la propriété intellectuelle, etc. Toutes ces notions sont encadrées d'un point de vue juridique. L'ASR n'est certes pas juriste, ni avocat mais il ne peut ignorer sa responsabilité dans ce cadre.

Cette première bonne pratique peut se résumer ainsi : « En savoir assez pour ne pas en faire trop ».

[forum : annoter le chapitre]

Faire de la veille juridique

L'environnement dans lequel évolue l'ASR évolue de façon permanente à trois niveaux :

- technique : les mises à jour et les nouveaux logiciels ;
- des usages : les utilisateurs sont à la fois demandeurs et utilisateurs des nouvelles techniques et des fonctionnalités apportées au travers de celles-ci ;
- du droit : qui apporte plus ou moins rapidement des réponses d'ordre juridique.

L'ASR est la personne à laquelle les utilisateurs adressent des demandes informatiques. Ces demandes

sont souvent relatives à l'accès aux données professionnelles comme personnelles, et aux besoins de confidentialité et de disponibilité. Il est donc amené à y répondre avec le plus de justesse et de précision possible dans le cadre technique et légal. Et, pour ce faire, une bonne pratique est de se tenir au courant régulièrement et au besoin de se faire assister d'un professionnel du droit [27].

En résumé : « Un ASR informé en vaut deux ».

[forum : annoter le chapitre]

Disposer d'une boîte à outils juridiques

Cette boîte à outils est constituée de documents que l'ASR doit posséder et dont dépendent les missions qui lui sont confiées :

- la charte informatique (généralement annexée au règlement intérieur de l'établissement) ;
- la charte administrateur qui peut s'appliquer à la fois à l'ASR et à l'utilisateur, le premier ayant des droits privilégiés sur les systèmes de son unité et le second sur son ordinateur de bureau ou portable ;
- le guide des opérations de contrôle sur les postes ;
- une connaissance concrète de sa chaîne fonctionnelle ;
- les mentions légales sur les sites web.

Vous trouverez des informations utiles sur les sites cités en annexe [28].

En résumé : «Un bon ouvrier (ASR) a toujours ses outils ».

[forum : annoter le chapitre]

Ne pas faire ce que tu n'as pas le droit de faire

Cette bonne pratique repose tout simplement sur le bon sens. En effet, au même titre qu'une lettre avec une mention « personnel » ou « confidentiel » doit être donnée à son destinataire sans être ouverte, un courrier électronique ou un répertoire avec ces mêmes mentions n'a pas à être lu par l'ASR sauf dans des cas bien particuliers légitimes. Là aussi, la légitimité d'une demande de ce type faite après de l'ASR passe également par son bon sens.

En résumé, « Ne fais pas à autrui ce que tu ne voudrais pas qu'il te fasse ».

[forum : annoter le chapitre]

Ne pas être négligent fautif : Informer – Contrôler – Agir

Quelque soit son statut, l'ASR doit respecter les règles de responsabilité civile suivantes :

- Article 1382 du Code civil : « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer » ;
- Article 1384 du Code civil : « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde...* » ;
- Et particulièrement, l'Article 1383 du Code civil : « *Chacun est responsable du dommage qu'il a causé, non seulement par son fait, mais encore par sa négligence ou par son imprudence* ».

Cette bonne pratique nous paraît importante à détailler.

Informer

Les administrateurs sont tenus à une obligation de conseil « renforcé » auprès des utilisateurs. En effet, le conseil « renforcé » s'applique à trois domaines : le nucléaire, la chimie risque de type « SEVESO » et l'informatique. Les ASR peuvent émettre des alertes ou des mises en garde. L'alerte permet d'informer d'un problème bien défini, connu et réel. La mise en garde permet de signaler la possibilité d'un problème (hypothétique ou probable). La présence de certains mots-clés comme « alerte », « conseil » ou « mise en garde » dans un rapport, un message électronique et/ou dans une rubrique « informations » ou « sécurité » de l'intranet de l'unité peut avoir un poids utile en cas de contentieux ultérieur.

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. La politique de gestion des traces du CNRS a fait l'objet d'un document officiel disponible dans l'intranet du CNRS [16].

L'information peut porter, par exemple, sur les bulletins du CERT et CERTA [15] (en particulier les alertes), les statistiques de virus, de spams, de débits réseau, les migrations prévues, les interruptions de service pour maintenance, les coupures du réseau avec l'extérieur.

Bien entendu, d'un point de vue légal, il est nécessaire de prouver qu'on a bien dispensé l'information nécessaire et donc, il faut avoir les moyens de donner des preuves de l'information et de la communication que l'on a fournies. Cela peut prendre différentes formes comme par exemple, faire un rapport annuel d'activités, envoyer un message électronique ou tenir la rédaction d'une rubrique « informations » dans l'intranet notamment sur la sécurité.

Contrôler

Depuis la Loi pour la Confiance en l'Economie Numérique (LCEN), il apparaît que le droit des ASR à tracer les activités des services et leur utilisation dans le SI est total et complet : diagnostic, analyse, contrôle, maintenance préventive, identification des comportements illicites.

Les bonnes pratiques consistent donc, par exemple, à détecter les fonctionnements anormaux du SI 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, par exemple, des sondes d'un système de monitoring (*cf. annexe 2*) ;
- 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 pédopornographie 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.

Une attention particulière sera à observer pour tout ce qui touche les informations personnelles (contexte privé résiduel), tant en terme de diffusion du contenu que de diffusion d'information concernant un contenu suspect ! En effet, les informations personnelles ne peuvent être remises qu'à un officier de police judiciaire dûment habilité. En cas de doute, ne pas hésiter à contacter le Haut Fonctionnaire Défense (HFD) directement ou via la chaîne fonctionnelle.

Agir

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

En contrepartie, 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 qu'il prouve par exemple qu'il était en vacances, et qu'il n'y avait pas de redondance humaine prévue.

En conclusion, l'ASR est amené à faire preuve de vigilance, de perspicacité et de discernement. Il a un devoir de surveillance des systèmes et réseaux, et d'anticipation des problématiques à venir les concernant.

Pour cela, le triptyque d'ordre juridique à retenir est :

- INFORMER les membres de l'unité des risques liés à l'utilisation des systèmes et réseaux mis à leur disposition ;
- CONTROLER l'utilisation des ressources informatiques faites par ces membres ;
- AGIR en rappelant à l'ordre ceux qui s'éloignent des bonnes pratiques et proposer des mesures disciplinaires pour sanctionner les comportements abusifs.

En résumé : « Ne jamais oublier le triptyque : informer, contrôler, agir ».

[forum : annoter le chapitre]

Prouver que l'on fait bien son travail

Il ne s'agit pas vraiment de prouver que l'on est un « bon professionnel » mais plutôt de démontrer que l'on n'est pas dans le cadre de la négligence fautive, autrement dit, de pouvoir prouver que l'on applique bien la bonne pratique n°6 précédemment citée.

Pour cela, il est primordial de garder des traces des actions entreprises dans ce sens comme :

- l'historique de ses échanges par messagerie, en particulier les messages d'alerte, de conseil et de mise en garde ;
- la mise en place d'un système (*wiki* ou autres) où sont enregistrées les interventions réalisées ;
- la réalisation de rapports réguliers d'activités, à insérer si possible dans le rapport quadriennal du laboratoire et dans ses rapports d'activité en tant qu'agent.

En résumé : « ASR, pour vivre heureux, vivons non cachés ».

[forum : annoter le chapitre]

Connaître et utiliser la bonne chaîne d'alerte

Il est important pour l'ASR de connaître cette chaîne d'alerte car en cas de dysfonctionnement, voire de perturbation totale, il est un maillon essentiel auprès de sa direction et des tutelles pour remonter l'information.

Cette chaîne est très souvent propre à chaque établissement et, pour les unités mixtes de recherche dépendant de plusieurs établissements, une telle procédure est logiquement mise en place au niveau des directions pour définir la chaîne retenue dans le cadre des PSSI [6].

En résumé : « L'ASR est un maillon certes mais un maillon essentiel ».

[forum : annoter le chapitre]

Savoir coopérer avec les autorités compétentes

L'ASR peut être amené à répondre à des autorités extérieures telles la police, la gendarmerie, la CNIL et également à des autorités administratives qui ont la possibilité d'exercer leur droit de communication comme l'administration fiscale, l'administration des finances, les douanes, la DGCCRF (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes), l'AMF (Autorité des Marchés Financiers), le procureur de la République, le juge d'instruction ou le tribunal correctionnel, voire la DCRI (Direction Centrale du Renseignement Intérieur).

L'ASR avec l'appui de sa chaîne fonctionnelle, qu'il doit connaître et informer [29], devra s'assurer des modalités prévues légalement et apporter les réponses demandées ni plus ni moins.

En résumé : « Informer ou cautionner… il faut choisir ».

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 unité 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, etc.) et des outils pour perfectionner ses compétences par le biais de différents types de formation.

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 délai 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 à 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 des sources d'informations suivantes :

- la méthode « Getting Thing Done », de David Allen, plus connue sous l'acronyme GTD [30] ;
- le livre de Thomas Limoncelli « Admin'sys, gérer son temps » [31] ;
- le livre de François Delivré « Question de temps » [32] ;
- des formations suivies par les auteurs [33] ;
- le livre de Marion Sarazin « S'initier à la PNL » [34] ;
- le site de Rémi Bachelet, Maître de Conférences en science de gestion à l'Ecole Centrale de Lille [35].

[forum : annoter le chapitre]

Différencier les processus (ou opérations) des projets

Dans la gestion des différentes tâches réalisées au cours de la journée, il convient de différencier ce qui relève, d'une part des processus ou opérations, et d'autre part des projets.

Les différences entre les opérations et les projets sont résumées dans le tableau ci dessous [35] :

Opérations	**Projets**
Milieu : répétitif, organisation stable	Milieu : inconnu, innovant, organisation temporaire
Processus récurrent, décisions réversibles	Processus historique, décisions irréversibles
Incertitude faible : variables endogènes, actions encadrées	Incertitude forte, variables exogènes, non contrôlables, degré de liberté
Cash-flow positif, le fonctionnement dégage un bénéfice	Cash-flow négatif, il faut investir avant d'avoir un retour
Maintient les activités existantes, celles qui font vivre l'entreprise	Crée les futures activités qui assurent l'avenir de l'entreprise
Difficulté : intervenir rapidement en cas de blocage	Difficulté : gérer un saut dans l'inconnu complexe

Tableau 5 : Différences entre les opérations et les projets

Un processus ou opération est quelque chose de bien défini, routinier et bien encadré. La façon de gérer son temps dans le cas d'un processus ou d'un projet n'est pas la même : le projet va demander plus de réflexion et l'utilisation de méthodes nouvelles. Nous allons développer dans les parties suivantes quelques bonnes pratiques pour gérer ses processus, mener à bien ses projets et tenir sa planification.

[forum : annoter le chapitre]

Les processus

1.2.1 Le schéma du flux de travail ou la technique du cycle

La méthode GTD propose un schéma du flux de travail [30] 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 boîte d'entrée.

Ensuite pour chaque élément stocké dans cette boîte, 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 le 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 que 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 boîte 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 deux versions et réfléchir à leur impact par rapport au paramétrage du service effectif dans mon laboratoire ».

1.2.2 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, à la messagerie instantanée, 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.

1.2.3 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,…). 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,…
- automatiser l'envoi de courriels pour se rappeler les taches récurrentes mais manuelles : compacter une base de données, éditer le listing mensuel des machines infectées,…
- se déplacer systématiquement avec son organiseur, son stylo, ses clés, ses cartes d'accès est aussi une bonne habitude.

[forum : annoter le chapitre]

La gestion des projets

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'est définie. Ce n'est pas quelque chose de négatif en soi. Au contraire, cela correspond au tout début du projet, au moment où 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, soit on n'a pas de solutions. Le schéma ci-dessous nous donne quelques suggestions pour bien mener un projet :

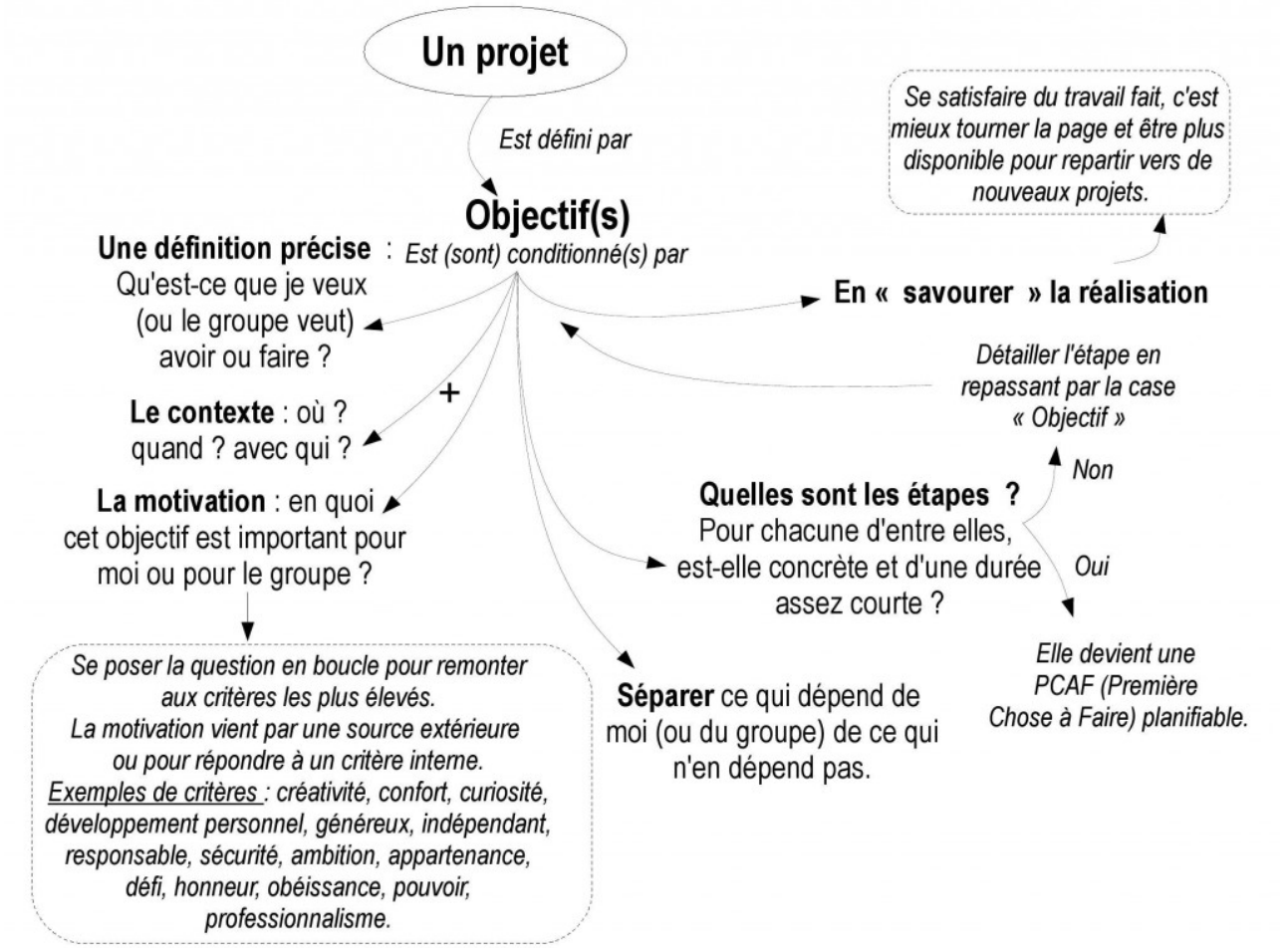


Figure 7 : Les suggestions pour bien mener un projet

Il s'agit pour commencer de préciser ce que l'on souhaite obtenir, dans quel contexte et d'évaluer sa motivation. Plusieurs allers/retours peuvent avoir lieu : en fonction d'un changement de contexte ou des critères de motivation, une redéfinition du projet est possible. Ensuite, une fois ces étapes réalisées, il s'agit de différencier ce qui dépend de soi ou du groupe et de définir les étapes concrètes.

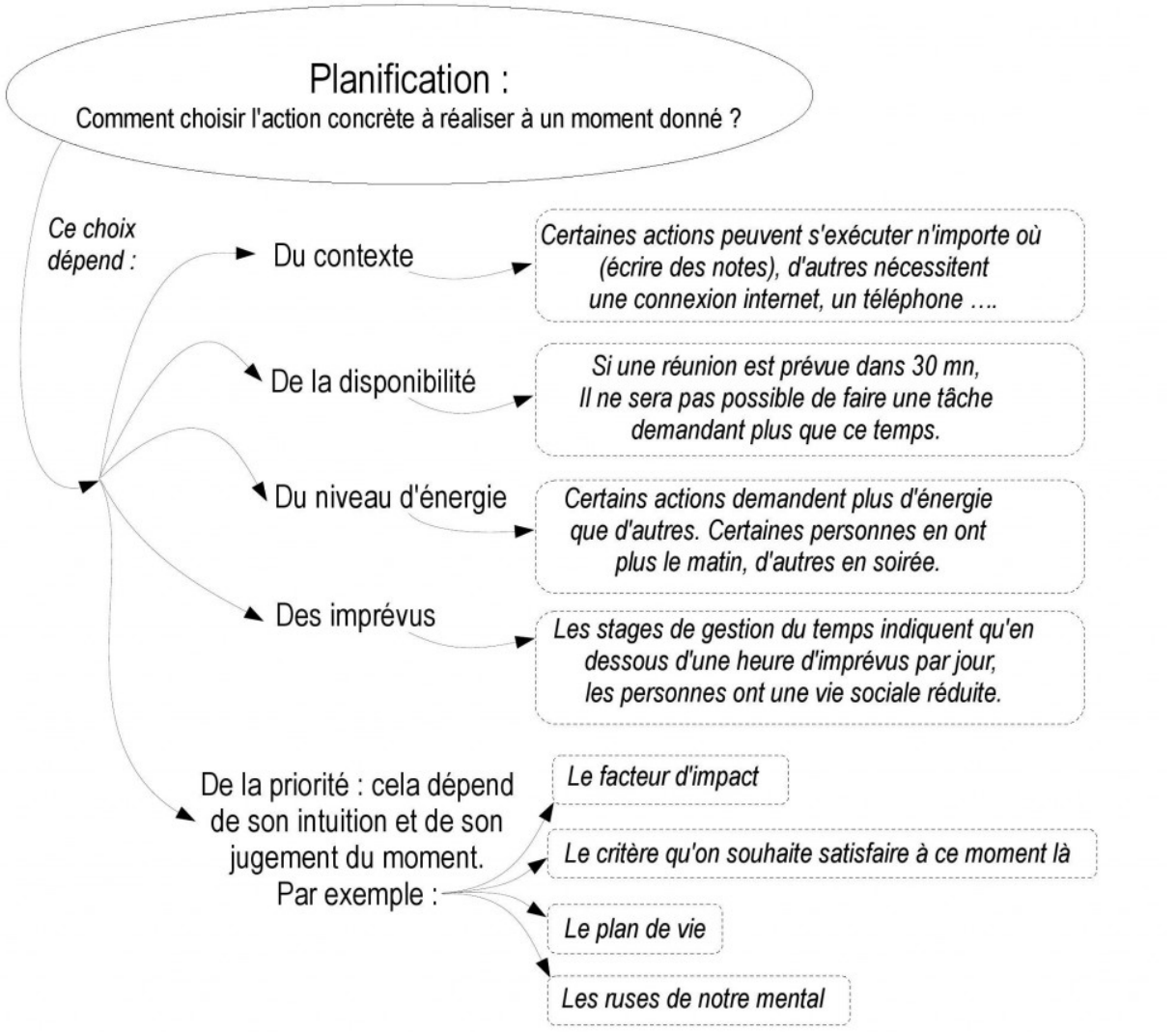
Le découpage en étapes plus simples et courtes est proposé par Thomas Limoncelli et David Allen. Ce dernier, avec la méthode GTD est plus concret dans le sens où il préconise de définir une première action (appelée PCAF) concrète et d'une durée assez courte. Lorsque le projet arrive à son terme, prendre le temps d'apprécier le travail réalisé est important pour passer à d'autres projets.

Pour plus d'informations, en particulier sur l'organisation et l'animation de projet et sur les outils à utiliser, vous pouvez consulter le site de Rémi Bachelet.

[forum : annoter le chapitre]

La planification

Le schéma ci-dessous résume les raisons qui nous amènent à choisir une tâche plutôt qu'une autre à un moment donné.



:

Figure 8 : Les choix possibles lors de la réalisation d'une action planifiée

Parmi ces choix, il y a la priorité et concernant celle-ci, plusieurs exemples sont donnés ci dessus :

- le facteur d'impact. 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 critère que l'on souhaite satisfaire à ce moment-là. Des exemples de critères sont donnés dans le schéma « gestion de projets ». Les 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 ») [32]. 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 ;

- le plan de vie. Il s'agit de passer d'un état où l'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 (voir le résumé [30]). 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 ;

- les ruses de notre mental. Nous en sommes parfois victimes et cela rend la gestion de notre planification difficile. Nous n'avons pas nécessairement conscience par exemple, d'être systématiquement tenté de sous-estimer le délai d'une tâche, de se disperser, de la peur des responsabilités, de l'hésitation perpétuelle. François Delivré les appellent les « diablotins » dans son livre. Il en recense une bonne dizaine. En prendre conscience, là aussi, peut nous aider à améliorer la gestion de notre temps [32].

[forum : annoter le chapitre]

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 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. Il ne faut pas être étonné si ces habitudes ne deviennent pas automatiques du jour au lendemain. Il faut être patient et apprivoiser ces techniques de manière progressive.

[forum : annoter le chapitre]

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 (forme écrite, orale, contractuelle, dialogue, écoute, 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 d'information, 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 SI ;
- 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 SI. Enfin, une bonne communication permet d'assurer la bonne lisibilité des missions du service au sein de l'unité.

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.

[forum : annoter le chapitre]

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.

2.1.1 La communication sur les activités du service des SI

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 :

Commission informatique d'une unité :

Une « commission informatique d'utilisateurs » regroupant les principales fonctions de l'unité (chercheurs, enseignants, administratifs..) est une instance qui peut se prêter parfaitement à l'établissement et à la validation d'une politique générale de 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.

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. Ce livret 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 le caractère professionnel et technique de la fonction d'ASR.
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 et 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 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, quels sont les quotas disques disponibles par individu ;
- L'accès au service de réseau sans fil, à *Eduroam* ;
- la politique de sauvegarde des données ;
- l'accès aux moyens de calcul disponibles dans l'unité ;

- la salle libre accès, les logiciels disponibles et les horaires d'ouverture ;
- le service VPN pour accéder de manière sécurisée à ses données depuis l'extérieur du laboratoire ;
- …

[forum : annoter le chapitre]

Compte rendu d'activités annuel et/ou quadriennal :

Le compte rendu d'activités annuel 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 soient intégrées aux rapports d'évaluation des autorités de tutelle.

Pour exemple, on pourra y mettre :

- une synthèse du nombre et de la diversité des tâches d'assistance 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, évolution 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 ;
- …

En définitive, il permet de résumer et de présenter au grand jour l'ensemble des activités et des tâches réalisées par le service informatique et améliore donc la communication et la lisibilité du service informatique.

2.1.2 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 ? : faire connaître aux utilisateurs les moyens et les procédures mis en place pour satisfaire les demandes, comme par exemple :

- un Système de Suivi de Demande (SSD) ;
- un site web intranet propre au service informatique.

Il est nécessaire de bien expliquer quelles sont les procédures 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.

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 des demandes des utilisateurs en leur accordant 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, par exemple, inscrit leur demande sur l'outil de suivi de demandes. Autant que faire se peut, on évitera le jargon 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* » 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* » permet à l'ASR de se donner la possibilité de planifier et d'ordonnancer leurs exécutions, 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.

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 : ex: 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. Exemple : un agenda collaboratif va être installé ;
- les changements de configuration de certains services. Par exemple : 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* » fait gagner, par effet d'échelle, le temps nécessaire à la résolution de plusieurs problèmes individuels identiques.

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 qui doit nous permettre de 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 enquêtes de satisfaction, des commissions informatiques régulières avec la direction et les utilisateurs pour faire remonter un indice de satisfaction.

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 :

- 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, etc. 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 dépôt documentaire (voir la partie sur la documentation) permettant d'échanger toute la connaissance au sein du service en l'absence des autres membres du service.

2.1.3 Communication, collaboration avec les partenaires extérieurs

Le milieu de la recherche scientifique est par principe très ouvert sur 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, nombre de nos unités sont souvent hébergées par des tutelles différentes, ou encore, sont amenées à travailler avec des partenaires industriels.

Nos unités partagent donc souvent leur environnement technique avec d'autres partenaires, si bien que les limites du SI peuvent être floues ou mal définies. Il est donc nécessaire de pratiquer une large ouverture et communication avec ces partenaires relevant d'autres tutelles, ou industriels... 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 déploiement et de sécurisation du SI ;

- prendre en compte et respecter les règles de sécurité d'un partenaire lors de la connexion par des moyens nomades au SI.

Les circuits de communication sont également tournés vers l'extérieur. L'ASR 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 réunions avec par exemple :

- la direction du système d'information (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 de l'Université, s'il existe ou son équivalent le plus « proche » ;
- la CNIL ou toute autre autorité judiciaire qui pourrait requérir l'information ;
- s'insérer dans les listes des réseaux métiers locaux.

2.1.4 Les relations avec les fournisseurs et les achats

Nombre d'ASR lorsqu'ils occupent des fonctions de gestion de service sont amenés à utiliser les ressources financières de leur unité, pour le fonctionnement et pour les investissements du service informatique. Ces investissements peuvent, bien souvent, être onéreux (système de sauvegardes, systèmes 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 tout en respectant les règles d'achats des tutelles.

De nos jours, l'ASR doit souvent s'investir et avoir des compétences dans les « techniques » administratives de rédaction et de passation des marchés publics (rédaction des CCTP, CCAP, MAPA, PUMA…) ainsi que des qualités de relation et d'organisation pour contacter différents fournisseurs, obtenir des démonstrations, négocier des prix et savoir choisir entre des offres partiellement comparables.

[forum : annoter le chapitre]

Recommandations sur les compétences

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 dix ans, leurs rapports à l'informatique se sont modifiés 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 passant par le développement applicatif, la mise au point de processus d'acquisition expérimentaux ou encore la gestion et l'optimisation de grappes de calcul (domaine de l'informatique scientifique) et de plus en plus l'expertise sur le traitement et la qualité des informations manipulées.

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 et aux demandes des utilisateurs.

Outre l'évolution des techniques, les matériels et les logiciels arrivent également vite à obsolescence. Des compétences nouvelles sont alors nécessaires pour apprécier et choisir les outils qui vont correspondre aux besoins des utilisateurs. Compte tenu du taux de renouvellement (généralement faible), 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). Il existe des formations spécifiques 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 ici en présentant différents aspects de la « mise-à-niveau » des compétences.

En résumé, quatre voies complémentaires permettent à l'ASR de ne pas être dépassé par les évolutions technologiques :

- l'auto-formation ;
- la formation continue ;
- la veille technologique ;
- les relations métier.

[forum : annoter le chapitre]

L'auto-formation

Installer un nouveau système sur une machine de test, valider le paramétrage d'une configuration, etc. : faire soi-même expérimentalement « sur le tas » est une manière 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 erreurs que d'autres ont déjà rencontrées, mais de permettre d'aller plus loin et de faire partager cette expérience. C'est de la valeur ajoutée à l'expérience des autres.

Avoir à disposition une machine de test, voire une machine virtuelle pour 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 avec des ouvrages de librairie est aussi bien sûr une source d'acquisition et d'approfondissement de compétences importantes.

[forum : annoter le chapitre]

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 du 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 le 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) ou « Actions Nationales de Formation » (ANF).

Il est absolument nécessaire que l'ASR prévoie et définisse 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 l'unité est le cadre adapté à ces demandes.

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 les domaines couverts par sa fonction, 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 de l'observatoire des métiers pour apprécier les compétences requises et les compléter afin de devenir plus efficace et faire évoluer sa mission en faisant des propositions à son unité.

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 les Journées Réseaux [36]) ou des salons techniques, des journées thématiques ;
- consulter des sites spécialisés sur internet.

[forum : annoter le chapitre]

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 [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 de RENATER [37] ;
- serveurs de liste du CNRS [38].

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 Interdisciplinaires (MI) du CNRS qui regroupe les réseaux de métiers
[39], et en particulier à la fédération des réseaux d'ASR : RESINFO [40], PLUME [41] pour le CNRS et chez RENATER [37] 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 (voir annexe 2)
Formation continue	Interlocuteur local Interlocuteur délégation Interlocuteur université Plan de formation
Veille technologique	Revues Lettres de « news » Liste de sites Séminaires Congrès
Relation de métier	Liste de diffusion Réseau régional Journées thématiques Sites de fiches techniques

Tableau 6 : Ressources disponibles pour gérer ses compétences

Le métier d'ASR concerne directement ce que l'on nomme les Technologies de l'Information et de la Communication (TIC) du fait même de l'utilisation et la gestion de matériels informatiques et réseaux.

La production, l'usage et le traitement en fin de vie des TIC soulèvent des enjeux à l'échelle de la planète : raréfaction des métaux précieux et des énergies fossiles, pollutions, et émissions de gaz à effet de serre. Aujourd'hui les TIC émettent plus de gaz à effet de serre que l'aviation civile. Une modification des pratiques est de nature à réduire ces impacts et à améliorer les impacts sociaux.

L'identification des principaux leviers de changement est apportée par l'étude des résultats des analyses de cycle de vie (analyse multicritère et pour toutes les phases du cycle de vie d'un équipement ou d'un service). Ces analyses (dont l'étude est détaillée sur le site de EcoInfo [42]) montrent la prédominance des impacts de fabrication et de recyclage pour les postes de travail, des impacts voisins pour ce qui concerne les serveurs et la prédominance des impacts dus au papier et consommables dans le cas des imprimantes.

Nous développerons dans cette partie du guide un ensemble de recommandations liées directement à l'utilisation des TIC pour en limiter l'impact environnemental. Elles s'appuient sur ce qui est exposé dans le Guide ECO-INFO issu d'un groupe de travail de RESINFO et disponible sur le site de EcoInfo [42].

Ce chapitre a été écrit par Françoise BERTHOUD et Jean-Daniel Dubois et a été adapté au guide.

[forum : annoter le chapitre]

Comment réduire les impacts environnementaux ?

L'idée générale est de réduire la quantité d'équipements utilisés et d'optimiser leur fonctionnement. Le périmètre d'actions ira de l'ensemble du campus ou au moins du laboratoire ou groupement de laboratoires (consolidation, rationalisation) à la gestion des postes de travail en passant par la mise en œuvre de démarches d'achat éco-responsables, d'actions spécifiques au niveau de la salle informatique ou la formation et la sensibilisation des acteurs.

[forum : annoter le chapitre]

Mettre en place une politique volontariste « développement durable – greenIT »

Le succès d'une démarche « développement durable » nécessite l'appui de toute la chaîne de décision de l'organisme. Des choix, des orientations politiques devront être posés, des changements seront attendus parfois mineurs (insertion de critères environnementaux dans les appels d'offre), parfois avec des conséquences importantes en terme d'organisation (création d'une infrastructure régionale par exemple) ! Dans ce contexte, il est évident que non seulement la direction doit être impliquée, mais aussi l'ensemble des acteurs du dispositif.

[forum : annoter le chapitre]

Mesurer et définir des indicateurs

Lors de la mise en œuvre d'actions de développement durable, la mesure et l'affichage de résultats est un élément clé de succès de l'opération dans la durée. Les indicateurs choisis doivent être en lien avec les orientations politiques de l'établissement.

Par exemple, si la priorité se porte sur les gaz à effet de serre, il sera important que l'indicateur tienne compte de la consommation d'énergie (en Chine, par exemple) pendant la phase de fabrication des ordinateurs (ce qui n'est pas pris en compte en général et qui aboutit à des mesures contre-productives !). Des exemples d'indicateurs sont précisés dans la suite du texte.

[forum : annoter le chapitre]

Réduire les biens d'équipement en usage et en renouvellement

Il s'agit ici de poser un regard « développement durable » sur l'ensemble du système d'information. Dans l'idéal, cette approche devrait compléter une démarche qualité (ITIL [7]) qui inclurait donc la qualité de l'environnement et des conditions de vie des personnes impliquées à toutes les étapes des processus.

Il sera donc nécessaire dans un premier temps de dresser un état des lieux précis des équipements, logiciels, ressources humaines, services rendus, besoins, etc., puis d'accompagner les changements utiles :

- en optimisant la dimension matérielle (par exemple en réduisant le nombre de salles informatiques, en consolidant les serveurs de services, en augmentant la durée

d'utilisation des équipements...

- en améliorant la prise en compte des besoins afin d'éviter les effets de contournement (ni sous-dimensionnement, ni surdimensionnement) ;
- en proposant des solutions logicielles adaptées à des équipements « vieillissants » ;
- en ne renouvelant pas les imprimantes individuelles et en proposant des solutions centralisées.

Quelques exemples :
– les postes de travail obsolètes peuvent trouver une seconde vie en postes de travail virtualisés ;
– préférez les ordinateurs portables aux postes fixes ;
– utilisez les techniques de virtualisation de serveurs ;
– mutualisez les services et donc les serveurs.
Indicateurs (à service égal) :
– poids (kg) équipements acquis année n / utilisateur ;
– nombre d'équipements acquis année n / utilisateur ;
– volume (m3) de salle informatiques / utilisateur ;
– âge moyen des équipements (postes de travail) mis en décharge ;
– nombre d'imprimantes / utilisateur ;
– satisfaction des utilisateurs (note).

[forum : annoter le chapitre]

Acheter éco-conçu, fiable et solide

Lorsque l'achat d'un nouvel équipement ne peut pas être évité, les écolabels permettent de faciliter l'identification des matériels contenant le moins de substances toxiques, ayant été conçus pour être plus recyclables, bref, minimisant les impacts environnementaux au cours de toutes les phases de leur cycle de vie. Différentes catégories de labels ont vu le jour.

Les écolabels globaux couvrent l'ensemble du cycle de vie d'un matériel informatique, de sa conception à

son recyclage :

- « EPEAT » [43]. Pour évaluer les matériels, EPEAT s’appuie sur 23 critères obligatoires et 28 optionnels. Ces critères sont classés dans 8 catégories différentes :
- réduction / élimination des substances dangereuses ;
- choix de composants respectant l’environnement ;
- prise en compte de la fin de vie du matériel dès la conception ;
- durabilité du matériel ;
- réduction de la consommation d’énergie ;
- recyclage ;
- implication de l’entreprise dans une démarche de développement durable ;
- emballage.

Cet écolabel se décline en plusieurs niveaux en fonction du nombre de critères satisfaits (or, argent, bronze) : privilégier les niveaux argent et or.

- TCO [44] : cet écolabel s’est récemment étendu aux postes de travail dans une approche très globale. Cependant, peu d’équipement sont labélisés à ce jour ;
- Ecolabel européen [45] : peu d’équipements labélisés ;
- Blue Angel [46] : peu d’équipements labélisés mais il s’agit d’un écolabel avec contrôle systématique.

Les labels portés sur les économies d’énergie se focalisent uniquement sur la consommation énergétique des appareils :

- Energy Star [47]. Ce label est très largement utilisé dans le monde ; il indique que le matériel intègre des mécanismes qui réduisent sa consommation énergétique : ACPI, mode veille automatique de l’écran... ;

- 80plus [48]. Actuellement, la plupart des alimentations électriques équipant les ordinateurs du marché ne dépassent pas 60% d'efficacité. 40% de l'électricité consommée par le PC est donc dissipée sous forme de chaleur ! Pour être certifiée 80plus, une alimentation électrique doit délivrer au minimum une efficacité de 80%. Ce label se décline en quatre niveaux progressifs. Les serveurs achetés aujourd'hui devraient tous être du niveau platinium;

L'aspect matériel est lui aussi important. La fiabilité du matériel, par exemple, conditionne directement sa durée de vie (et donc son impact environnemental). Inciter à investir dans les extensions de garantie, conduira les utilisateurs à conserver leurs équipements pendant au moins toute la durée de garantie.

Les équipements (de type poste de travail) proposés dans le cadre des marchés CNRS sont tous labélisés. Les serveurs sont toujours proposés avec l'option d'alimentation performante. Tous les matériels sont proposés avec une extension de garantie à 5 ans (ce que nous recommandons fortement).

Indicateurs (à service égal) :
– % matériel EPEAT (Bronze, argent, or) ou équivalent ;
– % matériel 80PLUS (Bronze, argent, or) ;
– durée moyenne de garantie des matériels acquis.

[forum : annoter le chapitre]

Optimiser le fonctionnement des salles informatiques

L'optimisation des salles informatiques a fait l'objet d'un dossier complet, consultable sur le site EcoInfo [49].

En résumé, les grands volants d'actions se situent autour des propositions suivantes :

- diminuer le nombre de salles informatiques ;
- améliorer l'urbanisation de la salle en optimisant l'organisation des baies dans la salle informatique (allées froides / chaudes) ;
- optimiser le refroidissement (augmenter la température de consigne, réduire le volume d'air à refroidir, confiner l'air chaud, utiliser des sources d'énergie renouvelables, utiliser la chaleur produite, ne pas onduler ce qui n'est pas nécessaire…
- éteindre les serveurs non utilisés ;
- virtualiser les autres et donc réduire le nombre de serveurs ;

- organiser le stockage (en fonction de la consommation électrique des équipements et de la demande des fichiers), les différentes technologies permettent de mettre en place une véritable gouvernance des données.

La commission Européenne a proposé un code de conduite qui est largement décrit (et traduit) dans l’espace de documentation référencé ci-dessus.

L’idéal serait de se rapprocher (pour les datacentres de taille suffisante) le plus possible des préconisations. Quant à la question des très petites salles, l’idéal serait de mettre en place des structures d’hébergement communes, qui satisferaient aux mêmes critères.

Indicateurs (à service égal) :
– kWh / an / utilisateur (serveurs)

[forum : annoter le chapitre]

Sensibiliser les utilisateurs

La mise en place d’une politique de développement durable pour le SI va induire des changements de comportements de la part des utilisateurs. Il est indispensable d’accompagner ces changements et d’en expliquer les raisons, par des actions de sensibilisation régulières. Par ailleurs, une implication active des membres du laboratoire (par exemple en participant à la réflexion ou à l’analyse des indicateurs) augmente significativement les chances de succès.

Utilisation des postes de travail :

- ne pas activer l’écran de veille ;
- activer la mise en veille de votre équipement (temps préconisé : 10 mn) ;
- activer l’hibernation (ou mise en veille prolongée) après 60 mn d’inactivité. C’est le mode le plus économe en énergie qui permet de restaurer les applications ouvertes lors de l’arrêt ;
- et surtout…. ne pas céder au « besoin impératif » de renouveler le matériel plus que nécessaire : il est extrêmement rare que les applications utilisées sur le poste de travail justifient un renouvellement supérieur à cinq ans (durée correspondant à la garantie proposée dans le cadre des marchés enseignement supérieur/recherche).

Impression :

- imprimer uniquement les documents qui ne peuvent pas être lus à l’écran ;

- paramétrer l'ensemble des moyens d'impression en recto-verso et mode brouillon par défaut, tout en laissant la possibilité à l'utilisateur de modifier ces paramètres au cas par cas ;
- consolider les imprimantes individuelles à jet d'encre vers des imprimantes multifonctions départementales équipées d'un code ou d'un système de badge. Le système d'identification permet de ne déclencher l'impression que lorsque l'utilisateur récupère le document papier ;
- imprimer sur du papier recyclé, à défaut issu de forêts gérées durablement ;
- mettre en place un circuit de recyclage du papier et du toner ;
- utiliser la police Century Gothic qui consomme 30% d'encre en moins.

Indicateurs (à service égal) :
– kg papier acheté / utilisateur ;
– kg toner acheté / utilisateur ;
– KWh / an / utilisateur (postes de travail et périphériques) ;
– Go stockés / utilisateur.

[forum : annoter le chapitre]

Porter une attention particulière au devenir des Déchets d'Equipements Electriques et Electroniques (DEEE)

Lorsque vous confiez vos déchets à une société, il est important de lui demander les documents de conformité (autorisation préfectorale). Aucune société n'est actuellement en mesure de recycler l'ensemble des matières présentes dans un ordinateur. Les cartes électroniques doivent par exemple être traitées par l'une des cinq sociétés mondiales capables de recycler proprement les métaux précieux. Il s'agit donc, dans la mesure du possible, de vérifier que les différents éléments sont effectivement retraités proprement et au plus près du lieu d'enlèvement (limitation transports).

L'ambition de ce guide a été 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 Mr. 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 appuyés 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 [4] et ISO 27001 [5], dans l'optique générale de donner un cadre référentiel à nos pratiques de terrain, permettant de rendre compte de la meilleure façon et contribuant, à terme, à améliorer la qualité du service.

Attention : comme cela a été dit dans l'introduction et rappelé à plusieurs reprises, 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.

[forum : annoter le chapitre]

Un cadre général : promouvoir une démarche qualité

Ce Guide des Bonnes Pratiques, est en effet un document où nous avons 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, se complexifient et ne sont pas réellement explicitées dans les fiches métiers…

Il nous a donc semblé indispensable, dans le contexte actuel, d'élaborer un corpus de bonnes pratiques organisationnelles qui va contribuer à rendre plus « lisible », 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 unités de recherche et d'enseignement, elle a donc été une des lignes directrices mises 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 Système d'Information 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 nécessite une bonne organisation du travail.

Outre la possibilité de pouvoir améliorer de 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 à nos directions, nos tutelles et nos utilisateurs/clients.

- La sécurité du Système d'Information

Parmi les points importants à prendre en compte dans les pratiques des ASR figure la sécurité de nos infrastructures informatiques et du système d'information.

Cette sécurisation fait partie de nos préoccupations quotidiennes car au cœur du fonctionnement des structures de recherche et d'enseignement dont la 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 [5]. Il nous a donc paru indispensable de dégager les principales procédures spécifiques à la sécurisation de nos infrastructures.

- Aspects juridiques

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 et planifier au mieux nos actions. Pour ce faire, nous nous sommes appuyés sur les ouvrages et les méthodes

connus afin de proposer une organisation du temps.

- Veille technologique et formation

Nous avons insisté 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 les formations permanentes, et les journées organisées par les réseaux métiers ou structures locales des établissements.

La participation aux différents réseaux de métiers et manifestations qui y sont liées en font partie. L'ASR est une personne qui vit en réseau, au propre et au figuré.

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 s'avère donc essentielle.

- Aspects environnementaux

Les choix des matériels, des infrastructures et des comportements liés aux TIC ont des répercussions grandissantes dans plusieurs domaines environnementaux. Ces enjeux sont planétaires. Aussi quelques recommandations pratiques sont abordées afin d'en limiter l'impact.

[forum : annoter le chapitre]

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 d'une manière différée et si besoin partagée.

Par ailleurs, si l'on se réfère au contexte actuel dont la tendance est à la mutualisation des moyens tant matériels qu'humains et 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 ayons 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, complétez-le, pour faire le point dans vos activités ou

faire des propositions d'amélioration pour la collectivité.

La fédération de réseau de métier RESINFO [40] 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!

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

Site internet : http://www.resinfo.cnrs.fr

ANNEXES

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

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 possibilités 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 refixer des objectifs… Une manière de mettre en place un plan PDCA.

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,…) ?
- Qui arbitre en cas de désaccord, de difficulté ou de conflit sur la définition des besoins ?

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, libre ou commercial ?
- si outil maison : est-ce distribuable à d'autres établissements ?
- Est-ce basé sur un SGBDR ? Lequel ?
- quels sont les éléments gérés par votre outil ?
- utilisez-vous un ou des outils d'inventaire automatique ?
- Si oui, lesquels ?

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 quel outil vous appuyez-vous pour ces enregistrements ?
- logiciels de gestion de configuration : CVS, subversion, Trac ?
- journaux de bord manuels, électronique ?

- autre méthode
- Comment se fait le partage des connaissances au sein de l'équipe des ASR (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 ?

Documentation pour les utilisateurs, Communication

- Quels sont les principaux éléments couverts par cette 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 système d'information ?

- évolutions, arrêts pour maintenance, incidents,…

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 compte ?
- 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 ?

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, -…) ?
- 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 ?

Gestion de la continuité de service

- Avez-vous mis en place des systèmes "haute disponibilité" pour assurer une

redondance ? Lesquels ? 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 ?

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 recherche ?
- Participez-vous au montage des dossiers CPER, ANR…. ?

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 ?

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…

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 REFERENCE

Nous avons répertorié ici des outils logiciels essentiellement issus du monde « Open Source », et de références bibliographiques pouvant illustrer et être utilisés dans les différents chapitres de ce guide des bonnes pratiques.

LA FOURNITURE DE SERVICES INFORMATIQUES

Une démarche qualité dans les unités de recherche

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 https://www.ocsinventory-ng.org/, Fiche Plume : https://www.projet-plume.org/fr/fiche/ocs-inventory-ng)
- Cfengine : administration automatisée de systèmes hétérogènes (Site web : https://www.cfengine.org/, Fiche Plume : https://www.projet-plume.org/fiche/cfengine
- Puppet : automatisation d'un grand nombre de tâches d'administration : installation de logiciels, de services ou encore modifier des fichiers https://puppetlabs.com/
- bcfg2 : Administration centralisée de serveurs https://bcfg2.org/
- Quattor : déploiement et gestion de configuration de machines Linux (Site web https://www.quattor.org/index.html
  - Fiche plume : https://www.projet-plume.org/fiche/quattor)
- Active Directory : mise en œuvre d'annuaire pour Windows (https://fr.wikipedia.org/wiki/Active_Directory)
- Exemple de procédure d'ouverture de compte (exemple-fiche-creation-compte-info)

La gestion des niveaux de service

On trouvera ici des outils pour mesurer le niveau de service offert aux clients du système

d'informations.

GLPI fournit des statistiques d'intervention qui permettent de mesurer le temps passé sur les demandes des utilisateurs, helpdesk associé à un outil de gestion (Site web https://glpi-project.org/fr, Fiche Plume : https://www.projet-plume.org/fiche/glpi)

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 (https://www.cacti.net/)
- Ntop : sonde réseau qui permet de remonter et analyser le trafic réseau sous forme de graphe (https://www.ntop.org/)
- Nagios : logiciel de supervision de réseaux et de systèmes (serveurs et postes de travail.) (https://www.nagios.org/)
- Centreon fournit une interface graphique pour permettre la consultation des informations issues de Nagios. (https://www.centreon.com/)

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 (https://www.linux-ha.org/)
- 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 : RESINFO

- Xen (https://www.xen.org/)
- Vserver (https://linux-vserver.org/Welcome_to_Linux-VServer.org)
- openVZ (https://wiki.openvz.org/Main_Page)
- Proxmox : cluster de serveurs openVZ (https://pve.proxmox.com/wiki/Main_Page)

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 (https://otrs.org/)
- GLPI : helpdesk associé à un outil de gestion (Site web : https://www.glpi-project.org/, 2. Fiche Plume : http://www.projet-plume.org/fiche/glpi)
- Request Tracker (RT) : gestion de tickets d'incidents (https://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 (https://www.esup-portail.org/display/ESUP/2008/08/22/esup-helpdesk+v3, https://www.esup-portail.org/display/PROJHELPDESK/esup-helpdesk+-+user+support+at+establishment-level)

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 : https://www.mantisbt.org/, Fiche plume : https://www.projet-plume.org/fr/fiche/mantis)
- Bugzilla : outil de gestion de bugs (https://www.bugzilla.org/about/)
- Gnats : outil de gestion de bugs (https://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 » (https://www.mondorescue.org/)
- System Imager (https://wiki.systemimager.org/index.php/Main_Page)
- PartImage (https://www.partimage.org/Page_Principale)
- JeDDlaJ (Le teaser)

La gestion des changements et de la mise en production

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.)
    - (The ELOG Home Page (psi.ch))

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

Le catalogue de services

- https://www.itilfrance.com/pages/docs/hgelun/itilv2_nivservice.pdf
- https://www.itilfrance.com/index.php?pc=pages/docs/index_pratique.inc&pg=menu_pratique.inc&ps=&pt=La%20biblioth%E8que%20-%20La%20pratique&pb=haut_entete_pratique.inc
- https://2011.jres.org/archives/14/index.htm, un exemple dans l'OSU Pytheas

La documentation

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

- Comparatif de wikis : (https://www.wikimatrix.org/compare/DokuWiki+PmWiki+TikiWiki+TWiki)
- PMWiki (https://www.pmwiki.org/wiki/PmWikiFr.PmWikiFr)
- MediaWiki (https://www.mediawiki.org/wiki/MediaWiki/fr)
- DokuWiki (https://www.dokuwiki.org/)
- TWiki (https://www.twiki.net/)

Les gestionnaires de contenu web (CMS) :

- Comparatif de serveurs de contenus (https://2007.jres.org/planning/pdf/104.pdf)
- Drupal (https://drupalfr.org/)
- Spip (https://www.spip.net/)
- Joomla (https://www.joomla.org/)
- WordPress (https://fr.wordpress.org/)
- eZ Publish (https://fr.wikipedia.org/wiki/EZ_Publish)

LA GESTION DE LA SECURITE

- [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] : formation A3IMP de l'UREC (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/fr/documentation/Guide_effaceur_V1.12du040517.pdf)
- [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

- 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 à 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
  - 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/
  - NetDisco : http://netdisco.org/, http://en.wikipedia.org/wiki/Netdisco
  - NfSen : http://nfsen.sourceforge.net/
  - smokeping : http://oss.oetiker.ch/smokeping/

LES ASPECTS JURIDIQUES DU METIER D'ASR

- 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 déclarée 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.dgdr.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.
- Le site internet legalis (http://www.legalis.net) vous permet d'accéder à des comptes rendu des jurisprudences de différents tribunaux.

LES CONTEXTES PERSONNEL ET RELATIONNEL

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 :
- Une vidéo de 4mn qui résume la méthode : https://www.youtube.com/watch?v=C0-Mva5fw1c
- Plus connue sous l'acronyme GTD, sur wikipédia : http://fr.wikipedia.org/wiki/Getting_Things_Done
- Un résumé de la méthode GTD par chapitre : http://gagnermavie.com/balade-a-travers-getting-things-done-chapitre-par-chapitre/
- Une comparaison des logiciels mettant en œuvre la méthode GTD : http://fr.wikipedia.org/wiki/Comparaison_de_logiciels_GTD
- Un logiciel de gestion de tâches à effectuer : 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
- [GPLI], [RT], [Esup-Portail], [HelpDesk] : voir les références données dans le chapitre 5 « Gestion des interventions ».

Recommandations sur les compétences

Des liens utiles de réseaux de métiers

[UREC] : https://aresu.dsi.cnrs.fr/

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

- [CCM] : http://www.commentcamarche.net/
- [Zero] : http://openclassrooms.com/
- [Resinfo/Josy] : http://www.resinfo.org
- [CUME] : http://www.cume.fr
- [Renater] : http://www.renater.fr
- Liste par thème tous les magazines qui paraissent : www.journaux.fr
- [TDLP] : Linux documentation Project http://www.tdlp.org/
- [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/
- [InternetActu] : http://www.internetactu.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 no 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 6o de l'article 34 de la loi du 11 janvier 1984 susvisée.

- Le contenu des formations prévues au 1o 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 leurs 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

FICHES CONCERNANT LES ASPECTS TECHNIQUES SPECIFIQUES A 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/sam/en/us/systemcenter.aspx) est la gamme Microsoft d'outils et logiciels pour l'administration des systèmes d'information. 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 composants, 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 installée 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…). Il est téléchargeable sur le site de Microsoft.

- Et enfin pour tous les utilisateurs avertis : https://technet.microsoft.com/fr-fr/sysinternals/bb545021.aspx
- La collection d'utilitaires SysInternals créée par Mark Russinovich et Bruce Cogswell et rachetée depuis par Microsoft constitue une mine d'outils totalement indispensables pour des systèmes sous Windows : utilitaires disques, utilitaires réseau, utilitaires de ressources et de processus, utilitaires de sécurité…

[1] J.L. Archimbaud, F. Berthoud, T. Dostes, M. Libes, N. Neyroud, J. Prévost, A. Rivet, « Le Système d'Information dans un laboratoire de recherche: guide de spécification des services », JRES, Strasbourg, 2007 (http://www.resinfo.org/spip.php?article11)

[2] Ecoinfo : 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 (http://ecoinfo.cnrs.fr/)

[3] ISO 9001 : Systèmes de management de la qualité – Exigences, Ed. AFNOR, 2008. (https://www.iso.org/fr/iso-9001-quality-management.html)

[4] ISO 20000 : Technologies de l'information — Gestion des services — Partie 1: Spécifications-Partie 2: Code de pratique, Ed. AFNOR, 2005 (https://www.iso.org/fr/standard/51986.html)

[5] ISO 27001 : Technologie de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences, Ed. AFNOR, 2005 (https://www.iso.org/fr/standard/41933.html)

Alexandre Fernandez-Toro, *Management de la sécurité de l'information,* Collection Solutions d'entreprise, 2ème édition, décembre 2009, Editions Eyrolles.

[6] PSSI : Politique de sécurité du Système d'information du CNRS 2007 (https://www.dgdr.cnrs.fr/bo/2007/01-07/416-bo0107-pb0.htm)

[7] ITIL : Information Technology Infrastructure Library, (http://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library, http://www.itilfrance.com/)

[8] Roue de Deming (http://fr.wikipedia.org/wiki/Roue_de_Deming)

[9] 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 (http://fr.wikipedia.org/wiki/Syst%C3%A8me_de_gestion_de_contenu)

[10] 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 (http://fr.wikipedia.org/wiki/Wiki)

[11] 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).

[12]

https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

[13] Méthode d'analyse de risques des systèmes d'information
https://www.ssi.gouv.fr/entreprise/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[14] 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.pdft

[15] Centre d'Expertise gouvernemental de Réponse et de Traitements des Attaques informatiques
https://www.cert.ssi.gouv.fr/

[16] Politique de gestion des traces du CNRS :
https://services.renater.fr/ssi/_media/securite/gestiondestraces-v2.6.pdf

[17] Journaux Systèmes : gestion des traces informatiques – problématique de centralisation des journaux et des traces informatiques : https://archives.jres.org/_media/tuto/tuto7/syslog-ng-tutojres.pdf

[18] https://securite-si.cnrs.fr/ et
https://intranet.cnrs.fr/protection_donnees/donnees/Pages/default.aspx

[19] https://www.ssi.gouv.fr/administration/bonnes-pratiques/cryptographie/

[20]
https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf

[21] http://www.legifrance.gouv.fr/initRechCodeArticle.do : faire une recherche sur le code civil et l'article 1316-1, ensuite sélectionner Livre III, Titre III, Chapitre VI, Section 1, Paragraphe 1.

[22] http://www.resinfo.cnrs.fr/spip.php?article47

[23] lien:
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=E607348D4A049DC1032EB2BFA17BBFAA.tpdjo10v_2?cidTexte=JORFTEXT000022683377&categorieLien=id

En particulier, l'article 89 :

« L'administrateur de la sécurité d'un système

Pour chaque système d'information traitant d'informations classifiées, l'autorité responsable de l'emploi du système désigne un administrateur de la sécurité pour mettre en œuvre les mesures opérationnelles de sécurité. A cet effet, l'administrateur est notamment chargé, en liaison avec l'ASSI concerné :

—de l'installation des logiciels correctifs de sécurité et des logiciels de protection ;

—de la gestion des moyens d'accès et d'authentification du système ;

—de la gestion des comptes et des droits d'accès des utilisateurs ;

—de l'exploitation des alertes de sécurité et des journaux de sécurité.

L'administrateur rend compte à l'ASSI de toute vulnérabilité du système qu'il détecte, de tout incident de sécurité et de toute difficulté dans l'application des mesures de sécurité.

L'administrateur de la sécurité doit, dans la mesure du possible, être distinct de l'administrateur du système. Il doit être habilité au niveau de classification des informations traitées par le système et au minimum au niveau Secret Défense. »

[24a] Guide pour les employeurs et les salariés :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf

[24b] guide relatif à la sécurité des données personnelles :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf

[25] http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1182

« La préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait – de la même façon que la poste doit réagir à un colis ou une lettre suspecte. Par contre, la divulgation du contenu des messages, et notamment du dernier qui concernait le conflit latent dont le laboratoire était le cadre, ne relevait pas de ces objectifs. »

[26] http://www.alain-bensoussan.com/wp-content/uploads/248807.pdf

[27] Le site du CRU (Centre de Ressources Universitaire) http://www.cru.fr offre un intranet juridique SSI (https://services.renater.fr/ssi/) dans lequel sont disponibles les lettres électroniques hebdomadaires du cabinet BENSOUSSAN. Vous pouvez y accéder avec votre certificat (CNRS, Universités…) ou demander un login au RSSI de votre établissement.

[28] • La Direction des Affaires Juridiques (DAJ) du CNRS http://www.dgdr.clfs.fr/daij/Default.html en particulier, quelques réflexes juridiques sur la création d'un site internet http://www.dgdr.cnrs.fr/daj/

• Un bon exemple à lire : Les mentions légales du site web du cabinet Bensoussan : http://www.alain-bensoussan.com/notice-legale/

et http://www.alain-bensoussan.com/politique-cookies/

• L'organisation de la SSI dans les établissements de l'Enseignement Supérieur et de la Recherche (http://www.cru.fr/ssi/securite/index) en particulier l'annexe juridique (http://www.cru.fr/ssi/_media/securite/sdssi-annexe2-juridique.pdf) sur la protection des données, des personnes, des droits de propriété intellectuelle, des SI, des correspondances, etc.

• Un exemple de charte « utilisateur administrateur » : http://www.resinfo.org/IMG/pdf/charte_user_adm_-_V6b.pdf

Sur les sites du CNRS :

• La charte informatique : http://www.dgdr.cnrs.fr/daj/publi/docs/Charte-informatique.pdf

• La Direction des Systèmes d'Information du CNRS : http://www.dsi.cnrs.fr/

• La sécurité et la protection du patrimoine scientifique au CNRS : http://www.dgdr.cnrs.fr/FSD/

[29] Que faire en cas de d'incident SSI ? : http://www.dgdr.cnrs.fr/FSD/securite-systemes/que-faire1.htm

[30] David Allen, *Getting Thing Done*, 2001. Son livré décrit une méthode de gestion des priorités quotidiennes. Un résumé de 7 pages du livre de David Allen : https://gbp.resinfo.org/wp-content/uploads/2021/10/GbpFichePratiqueGestionduTempsDavidAllen.pdf

[31] Thomas Limoncelli, *Admin ' sys, Gérer son temps*, traduit par Sébastien Blondeel, Editions Eyrolles : http://www.editions-eyrolles.com/Livre/9782212119572/admin-sys

[32] François Délivré, *Question de temps*, consultant en relations humaines et organisation, spécialisé dans le coaching des cadres dirigeants. Un résumé de son livre est disponible ici :https://gbp.resinfo.org/wp-content/uploads/2021/10/Resume-du-livre-de-Francois-Delivre-_Question-de-temps.pdf

[33] • Formation à l'encadrement de 7 jours réalisé par l'Institut Normand de Ressources individuelles et sociales : http://www.inris.fr/

• Formations sur les outils de communication, d'écoute et d'efficacité personnelle de 21 jours par la société Communication Active Normandie : http://www.communication-active-normandie.fr/

[34] Marion Sarazin, *S'initier à la PNL*, Série Développement personnel, ESF éditeur. Marion Sarazin a occupé pendant 20 ans des fonctions de direction d'entreprise. Elle a obtenu a obtenu un master en psychologie à l'université américaine de Santa Clara et est maintenant psychothérapeute https://www.lalibrairie.com/livres/s-initier-a-la-pnl–les-fondements-de-la-programmation-neurolinguistique_0-1209897_9782710122456.html

[35] Rémi Bachelet est Maître de Conférences à l'Ecole Centrale de Lille sur, entre autres, la gestion de projets et les méthodes de résolution de problèmes. Son site est disponible à cette adresse : http://rb.ec-lille.fr/gestion_projet.htm.

[36] http://www.jres.org/

[37] https://groupes.renater.fr/sympa

[38] http://listes.services.cnrs.fr/wws

[39] https://www.cnrs.fr/mi/spip.php?article465

[40] http://www.resinfo.cnrs.fr/

[41] http://www.projet-plume.org/

[42] http://www.ecoinfo.cnrs.fr

[43]https://fr.wikipedia.org/wiki/EPEAT

[44] https://fr.wikipedia.org/wiki/Certification_TCO

[45] https://www.ecolabels.fr/quest-ce-quun-ecolabel/

[46] https://www.greenit.fr/blue-angel/

[47] https://fr.wikipedia.org/wiki/Energy_Star

[48] https://fr.wikipedia.org/wiki/80_PLUS

[49] https://ecoinfo.cnrs.fr/2020/05/19/guide-des-bonnes-pratiques-du-code-de-conduite-europeen-sur-les-datacentres/