Contexte juridique des ASR – où en est-on? (*) Guide des bonnes pratiques des ASR (**)

Maurice Libes

et la production de 2 groupes de travail

(*) virginie Collomb
magalie Contensin
martine Culioli
thierry Dostes
kai Poutrain

(**) olivier Brand-Foissac
laurette Chardon
marie David
gilles Requilé
alain Rivet

Le Contexte...

- Nombre d'incidents de sécurité sur la DR12 au printemps 2006
  - Phishing sur patchs de sécurité « horde » passés trop tard
  - Compromission de serveur web sur Scripts PHP faisant des « include » de fichiers dans l'URL
  - Téléchargements intensifs dans la DR

- mise en cause de la protection des données sensibles du laboratoire et donc ? la responsabilité de l'ASR *in fine... ?*

Le Contexte

- Nécessité de porter plainte pour se couvrir
  - Y a t'il faute?
  - De quoi sommes nous responsables juridiquement? *(dixit un asr en colère..)*

- Le but n'est bien entendu pas de vouloir se dégager de nos responsabilités mais de mieux les appréhender et d'en préciser le périmètre afin d'adapter notre comportement face aux risques juridiques encourus.

Le Contexte...

- Certaines chartes informatiques d'établissements, stipulent en effet que « tout ASR a le droit d'être informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible »

- D'autant que la PSSI CNRS énonce que (p.7) :
  - Protection juridique : la mise en oeuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire ... Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée

Un éventail des principales questions

- *Eclaircissement sur la portée juridique des documents qui nous sont communiqués ...obligation de résultats? (Chartes, guides, décrets, circulaires, recommandations, délibération)*
- *Responsabilités respectives de l'ASR, du CSSI? vis à vis du Directeur d'unité*
  - *concernant le traitement des avis de sécurité et de l'application de la SSI*
- *Responsabilité de l'ASR vis-à-vis de l'exploitation des données et de leur sauvegarde*
  - *perte de données ?*
  - *Sauvegardes ?*
  - *Quelles prérogatives dans la gestion des données des comptes utilisateurs ?*
  - *Quelles prérogatives vis à vis de la sphère privée des utilisateurs ?*

Un éventail des principales questions

- *Responsabilité et attitude vis-à-vis de la découverte de contenus illicites*
- *Droit d'utiliser outils intrusifs sur postes clients? OCS, VNC?*
- *Responsabilités vis-à-vis de l'exploitation du parc de PC et de la sécurité du réseau local*
  - *droit de refuser de connecter un poste « nomade » au réseau s'il ne répond pas aux exigences de sécurité, et selon quelle procédure ?*
- *Responsabilités vis-à-vis de la disponibilité du SI et de la continuité de service?*
    - *Doit-on assurer une continuité de service? Responsabilité si patch non appliqué dans les temps ?*
- *Canal de communication entre ASR et Personnels du Laboratoire*
  - *Comment bien communiquer au sein du labo? Prouver officiellement que des actions de sécurisation ont été faites*

Objectifs ?

- Notre groupe de travail a essayé de formaliser les questions principales que nous nous posions, avec l'objectif :
- 1. d'obtenir des réponses de nos tutelles, préciser les implications juridiques et pénales du métier d'ASR
- 2. d'organiser une formation avec un juriste qui pourrait y répondre

- *3. aboutir à la rédaction d'un « document cadre » qui préciserait les droits et devoirs d'un ASR ?*
  - Sous une forme qui ne nous soit pas opposable
    - *Charte, livre blanc? Guide des bonnes pratiques?*

Objectifs

- Notre document de questions a donc servi de cahier des charges pour une formation confiée à un juriste
  - en janvier 2008 lancée avec la FP de la DR12
  - (Me E. Barbry, cabinet Benssoussan) , spécialiste de la SSI

- => Cet exposé reprend la synthèse de cette formation juridique , que nous avons rédigée laurette Chardon (DR19) et moi même
  - (document disponible pour qui le souhaite)

  - *NB : je ne suis pas juriste, je retransmets ici ce que j'ai compris et retenu de cette formation en tant qu'ASR ;-)*

Responsabilité juridique ASR où en est-on?

- Quelle est la place de l'ASR dans la SSI? Que dit la PSSI du CNRS? Page 20 on parle de l'administration des serveurs.. on serait donc « responsable » de l'administration des serveurs.. point !
- Pas plus d'information dans la charte utilisateur du CNRS, ni dans les textes du CNRS. Les responsabilités de l'ASR sont donc assez mal définies et écrites...
- ... mais il existe pourtant un cadre juridique
  - ex page 7 la PSSI dit que :
  - ***« Protection juridique :*** *la mise en oeuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle et industrielle et ceux de la vie privée (fichiers nominatifs, cybersurveillance…). Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée.* «

Responsabilité juridique ASR où en est-on?

- De 2002 à 2007 on assiste a une explosion du Droit en matière de SSI (LSI, LSQ, LSF, LCEN...). De nombreuses entreprises dont le CNRS, sont amenées à créer leur propre PSSI
  - Depuis 2004 : une nouvelle « ère juridique » : on assiste à un renforcement des condamnations

- Le maître mot et l'objectif premier de cette formation était de connaitre : *Quelles sont nos responsabilités juridiques dans l'exercice du métier ASR ?* ».
  - Le Problème ne se pose pas exactement en ces termes ! Mais plutôt plutôt en termes de :
    - savoir où se situe la Responsabilité en terme de Droit dans notre métier d'ASR et dans la SSI, et que signifie t-elle?
    - être *sensibilisé à la « Responsabilité »* relative à la SSI

Panorama de la responsabilité en SSI

- Comme préambule:

- Il ressort de la formation reçue qu'il n'y a :
  - aucune réponse définitive à ces questions de responsabilité
  - ni aucun glossaire précis des responsabilités qui nous incombent, ni des fautes que nous pourrions éventuellement commettre
- L'ASR se trouve en présence de différents « environnements juridiques ». Il faut parler du panel « des responsabilités » *eu égard à la Sécurité du Système d'Information*...

Panorama de la responsabilité en SSI

- *Responsabilité civile*
  - avec contrat : Loi des différentes « parties » : diffamation, contrefaçon etc...
  - hors contrat
- Responsabilité Pénale
- Responsabilité administrative
- Responsabilité personnelle
- Responsabilité partagée

- *Dans ce cadre de la SSI seules les responsabilité civiles et pénales sont couramment invoquées.*

- *Peu de cas de jurisprudence en responsabilité administrative dans le cadre de la SSI : surtout utilisée pour les sanctions disciplinaires. peu impliquée dans le cadre de la SSI...*

Panorama de la responsabilité

- La responsabilité civile (hors du cadre de tout contrat) est définie par les articles 1382, 1383 et 1384 du Code civil: la faute directe, la négligence fautive et la faute du fait des autres.
- **Art. 1382 :** *Tout fait quelconque de l'homme, qui cause un dommage à autrui, oblige celui par la faute duquel il est arrivé, à le réparer.*
  - *En cas de faute, il faut réparer le dommage (exemple : téléchargement 7j/7, lecture d'un mail privé)*

- **Art. 1383:** *Chacun est responsable du dommage causé non seulement par son fait, mais encore par sa négligence ou par son imprudence.*
  - *Cela concerne les fautes par négligence fautive ou l'imprudence de son propre fait*
    - Exemple de négligence fautive (= « laisser faire ») sur un SI : si un hébergeur a connaissance d'un contenu illicite et qu'il ne fait rien pour l'enlever *(jurisprudence Cyberlex)*

Panorama de la responsabilité

- **Art. 1384 :** *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.*
  - Exemple: employeur responsable des agissements de ses employés. Enseignants, artisans sont responsables des fautes des élèves, apprentis sous leur garde.
- La responsabilité de l'employeur est engagée lors d'un fait d'un salarié, lors d'un dommage ou d'un fait « commis dans le cadre de ses fonctions ». *(ex: jurisprudence "lucent")*

Responsabilité pénale

- Concerne les délits de :
  - *Contrefaçon, diffamation, Injures, Racisme, Révisionnisme, Incitation, ouverture correspondance privées, intrusion SI, Altération SI, Modification Suppression de données preuves, Mise à disposition, Enregistrement audio/vidéo sans autorisation, Diffusion et stockage d'image à caractère « pédo »..., non déclaration à la CNIL, pas de notices Légale sur site Web etc...*
- peu de recul jurisprudentiel en Droit Pénal en matière de SSI car les lois nouvelles datent de 2001, et un jugement complet dure environ 6 ans (affaire : 2ans, appel : 2 ans, cassation : 2 ans)

  - Lors de l'accès aux données des utilisateurs, L'ASR a obligation de Confidentialité... Mais a obligation de “dénoncer” eu égard au Droit Pénal si on découvre des données illicites concernant la pédopornographie , le révisionnisme etc.

Responsabilité personnelle

- La responsabilité personnelle pourrait être engagée dans quelques cas comme :
  - refus illégitime d'accomplir un acte, ou
  - manquement à une obligation.
  - Faute professionnelle
    - Exemple : si on télécharge massivement des données à titre personnel, notre responsabilité personnelle est engagée

Responsabilité partagée

- C'est le fait de déléguer une responsabilité pénale à quelqu'un.
  - Par exemple un chef d'Entreprise délègue sa responsabilité à un chef de chantier
- Il n'existe pas de délégation dans les organismes publics. L'ASR n'a pas de délégation pénale : il n'a pas la responsabilité de l'employeur au niveau pénal.
  - ==> un Directeur d'unité ne peut pas déléguer sa Responsabilité sur le plan Pénal

- Pour qu'il y ait délégation de responsabilité pénale : il faut un document signé par la personne qui accepte la délégation. La personne doit avoir l'autorité et les moyens.
  - L'acte de Délégation DOIT définir ce sur quoi on fait porter la Délégation !
- Si on n'a pas les moyens d'appliquer correctement une politique de sécurité, il faut l'indiquer PAR ECRIT! « Pour agir efficacement il me faut .... »

Responsabilité et SSI

- La donne est inversée en matière de responsabilité dans la sécurité des Systèmes d'Information :
  - i.e; un intrus n'est un intrus que si on lui a donné “conscience” d'être un intrus.

- En matière de SSI, pour sécuriser un espace privé il faut donc
  - *Bien entendu Sécuriser, mais aussi*
  - *signifier et mettre en place clairement les règles d'accès*...
  - et délimiter les zones protégées (vous êtes sur un site privé...)
- sans quoi un intru peut se réfugier derrière le fait de ne pas savoir qu'il était en terrain “privé”. *(ex: jurisprudence tati)*
  - Par exemple, dans un intranet, il faut que les pages soient marquées comme « appartenant à l'intranet » ou confidentielles.

Obligation d'informer, tracer et de sécuriser : Exemples de jurisprudence

- Jurisprudence IBM
  - *Problème grave dans le Si de flammarion suite à une mise à jour d'un logiciel par IBM..*
    - *Dans un domaine technique classé dangereux et dans une situation de danger, la partie la plus apte a "une obligation de conseil renforcée. »*
- Jurisprudence tati
  - Un individu rentre dans le Si de tati... prend possession d'un répertoire client... jugement : "aucune méthode de piratage mais une manipulation "accessible à tout internaute averti »
    - mauvaise sécurité du site, pas d'information, pas de frontière délimitant l'intranet... pas coupable!
- Jurisprudence lucent
  - Site web « escroca » établi par un employé de lucent pendant ses heures de travail...
    - Diffamation, et responsabilité de l'employeur, « non charte »

Obligation d'informer, tracer et de sécuriser : Exemples de jurisprudence

- Affaire “cyberlex” (? année)
  - site web de cyberlex «comment (ne pas) payer sur l'internet » citait des logiciels qui génèraient des numéros de cartes bleues bidon. Le site condamne ces activités mais donnait sur son site 2 liens sur 2 logiciels.
  - le magazine « Que Choisir » : cite l'article et l'auteur est cité comme un *!$?? ... Cyberlex demande au magasine "Que Choisir?" de retirer l'article ou d'avoir un droit de réponse.. qui est refusé.
    - Procès plainte pour diffamation contre plainte pour « contrefaçon »
  - Jugement : on est dans un cas d'imprudence et de négligence fautive de la part de Cyberlex qui avait laissé des liens vers des sites de pirates, qui malgré l'objectif pédagogique, ont été jugés comme une «incitation au délit»

Loi Informatique et Liberté, la CNIL

- On va devoir avoir des collaborations fréquentes avec la Police, la DST, la Justice, la CNIL

- La CNIL devient une autorité de contrôle hyper puissante !
  - La CNIL a désormais le pouvoir de faire une enquête
  - pouvoir d'opérer des vérifications sur place
  - pouvoir d'aller n'importe où dans le SI
  - pouvoir d'instrumentaliser la procédure
  - pouvoir de condamner à une amende

Loi Informatique et Liberté, la CNIL

- Plusieurs principes fondamentaux sont définis dans les lois de protection de la vie privée
  - Nécessité d'information des intéressés,
  - Nécessité de proportionnalité et loyauté des mesures prises,
  - Donner un droit d'accès et de rectification,
  - S'assurer de la durée limitée de conservation des informations à caractère privée, le droit à l'oubli.

Loi Informatique et Liberté, la CNIL

- Principes actuels :
  - tous les éléments qui sont dans un bureau d'un employeur sont réputés professionnels... De ce fait l'employeur peut y avoir accès même en l'absence du collaborateur
  - Tous les mails (messagerie électronique) sont réputés à caractère professionnel sauf si la mention [PERSONNEL] apparait dans le sujet
  - face à une situation de risque on « peut » ouvrir de la correspondance privée pour des raisons de sécurité ou d'urgence

- En cas de “doute” sur utilisation des moyens qui “dépassent” la vie privée résiduelle : La direction peut faire appel à un juge des requêtes : ordonne à un huissier une intervention en urgence (48h).

Loi Informatique et Liberté, la CNIL

- Quelque exemples : Cas du départ d'un personnel, que faire des données ?
  - il est légitime de basculer sa boîte de Mails d'une personne vers une autre.
  - Il est nécessaire d'informer et d'écrire dans les procédures d'ouverture et fermeture de compte que les données seront détruites ou transférées au Responsable au départ de l'utilisateur.
  - De même il est nécessaire d'indiquer ce qui sera fait du répertoire [PRIVE] dans le règlement
- Comment traiter une machine personnelle qu'on doit connecter dans le réseau du Laboratoire ?
  - La considérer comme un élément qui fait partie intégrante du SI du Laboratoire, elle suit le même régime... L'écrire dans le règlement

Loi Informatique et Liberté, Vie privée résiduelle

- ***notion de vie privée résiduelle :*** «espace» de vie privée au travail. Ex: C'est la possibilité de faire usage personnel de la messagerie et un dossier personnels.

- Au niveau du Laboratoire , il est nécessaire de *définir les règles du Jeu :*
  - mettre en place des éléments de distinction entre vie privée personnelle ou professionnelle
    - Ex: Indiquer le droit de brancher un portable personnel dans le réseau de l'entité? Avec contrôle? Sans contrôle?
  - Si contrôle : ils doivent répondre à des objectifs légitimes : exigence de sécurité, de prévention, gestion et optimisation des ressources, protection des intérêts de l'institution.

Conclusions : Les règles du jeu de la SSI

- Les “bonnes pratiques” dans le cadre juridique de la SSI pour se prémunir de responsabilités civiles et pénale est de mettre en place le *tryptique* :
  - *Information -> contrôle -> Action*
    - *Dans un contexte de faute, un juge analysera si on a “informé”, “contrôlé” et si on a “agit »*

- Nécessité cependant de PROUVER qu'on aura mis en place les éléments de la chaîne *Information/Contrôle/Action* ..... (preuves écrites archivées)
- Pb : dans nos milieux Universitaires et Recherche il y a une *faible culture de l'écrit administratif*. On ne trace pas beaucoup par écrit les actions qui ont été entreprises.

Conclusions : Les règles du jeu de la SSI

- il faut donc pour nous ASR tracer nos actions :
  - rubrique sécurité sur notre site Web, main courante...
  - rapport annuel d'activités
  - Montrer qu'on a informé et donc tout écrire :
    - faire des alertes des mises en gardes par des mails ou figurent les mots « Alertes » « Mises en garde »
- Principes à retenir
  - tryptique Information/Contrôle/Action
  - politique de l'écrit
  - traçabilité

Informer

- L'ASR, le RSSI se doit d'avertir, *de renseigner, d'informer, de mettre en garde*, aussi bien le responsable légal, les autorités compétentes, et surtout les utilisateurs, des risques dont il a connaissance de préférence par écrit
  - **Informer et former:** faire des rapports réguliers ou sur situation particulière de risque .

- Alerte et conseil: En tant qu'experts sur un domaine technique classé « dangereux » les ASR sont tenus à une *obligation de conseil renforcé*.
  - Il peuvent émettre des **alertes** (sur des risques connus) ou
  - des **mises en garde** (sur des risques possibles)...

- La ***présence de ces mot-clés*** CONSEIL, MISE EN GARDE, ALERTE dans un rapport peut avoir un poids utile en cas de contentieux ultérieur

Contrôler... tracer...

- Depuis la LCEN le droit à TRACER les utilisateurs dans un SI est *total et complet*
- *Participer au maintien de la preuve : Collaboration et coopération (cnil, dst..)*

- On n'a plus à se demander si on a le droit de mettre en place les outils de contrôle pour :
  - *Surveiller le réseau, les systèmes : outils de métrologie, de monitoring, de conservation et analyse des logs...*
    - *Respecter cependant la réglementation sur la conservation des traces et l'information et la vie privée résiduelle des utilisateurs*
  - Effectuer des statistiques sur le débit, les sites consultés, la consultation du site du labo, la place occupée sur les disques, ...
  - avoir des remontées en cas problème.
  - ...etc

Contrôler... tracer...

- Les contrôles doivent répondre aux obligations légales de sécurité et de traçabilité: *exigence de sécurité, de prévention, gestion et optimisation des ressources, protection des intérêts de l'institution*.
  - Ex: En cas de téléchargement massif par un utilisateur, l'ASR a le droit de stopper le flux réseau. On peut couper un service *sans plus se poser la question du droit de le faire*, mais en informant largement ... la Direction, les utilisateurs
- Si découverte de contenu illicite? :
  - en règle générale les administrateurs sont tenus au secret professionnel, mais ont l'obligation de dénoncer des actes délictueux: contenus illicites, notamment la pédo-pornographie ou la diffamation.

Agir, réagir...

- Préserver la sécurité du SI, maintenir la continuité de service :
  - empêcher que les données soient déformées endommagées *(intégrité)* ou
  - que des tiers non autorisés aient accès au SI *(confidentialité)*
  - *exécuter les patchs de sécurité*
  - *réagir vite pour enlever un contenu illicite « immédiatement ».*
- Droit d'agir en refusant des demandes qui mettraient le SI en danger.:
  - diagnostic, analyse, contrôle,
  - identifier des comportements illicites
  - maintenance préventive,

Guides des Bonnes pratiques des ASR

- Un groupe de travail constitué dans Resinfo
  - *olivier Brand-Foissac*
  - *laurette Chardon*
  - *marie David*
  - *gilles Requilé*
  - *alain Rivet*

Guide des Bonnes pratiques, pourquoi?

- Les PSSI sont très récentes, et les chartes ne stipulent que les droits et devoirs des utilisateurs au sens large.
- On note une ***absence forte de définition de poste d'ASR au CNRS comme à l'EN,*** il y a nécessité :
  - de travailler sur des lignes directrices (textes de lois existant et cas de juriprudence...)
  - D'améliorer « la visibilité du métier » en:
    - créant un « réseau de compétence », une émulation autour de la sécurité des SI
    - en réfléchissant à **une charte des ASR** ... tout en commencant par un Guide des bonnes pratiques, un document « fourre tout » où on mettrait toutes les spécificités du métier d'ASR.

Guide des Bonnes pratiques, pourquoi?

- 2 raisons d'avancer vers cela :
  - Élaborer un corpus de règles, de bonnes pratiques d'administration : Contribuer à rendre plus « lisible » les missions, l'organisation de nos services vis à vis de nos Directions et tutelles et utilisateurs
  - Avoir une "démarche qualité" d'amélioration continue du service
- *Le terme « **bonnes pratiques** » désigne, dans un milieu professionnel donné, un ensemble de comportements qui font consensus et qui sont considérés comme indispensables ... (wikipedia)*

GBP : objectifs groupe de travail resinfo

- Le terme "qualité" est utilisé ici en référence aux projets de "Démarche Qualité en Recherche" qui se développent dans nos laboratoires mais qui ne prenent pas en compte jusqu'à présent la spécificité du métier d'ASR.
  - Le projet de notre groupe de travail RESINFO à l'origine peut donc s'inscrire dans un cadre général de "Démarche Qualité"

- Référence nécessaire aux quelques standards et normes en vigueur utilisés dans le monde industriel (*ITIL ou ISO 20000*)
  - essentiellement pour se conformer à l'existant et fixer des repères identifiables, un langage commun dans la classification que nous proposons.

GBP : contenu

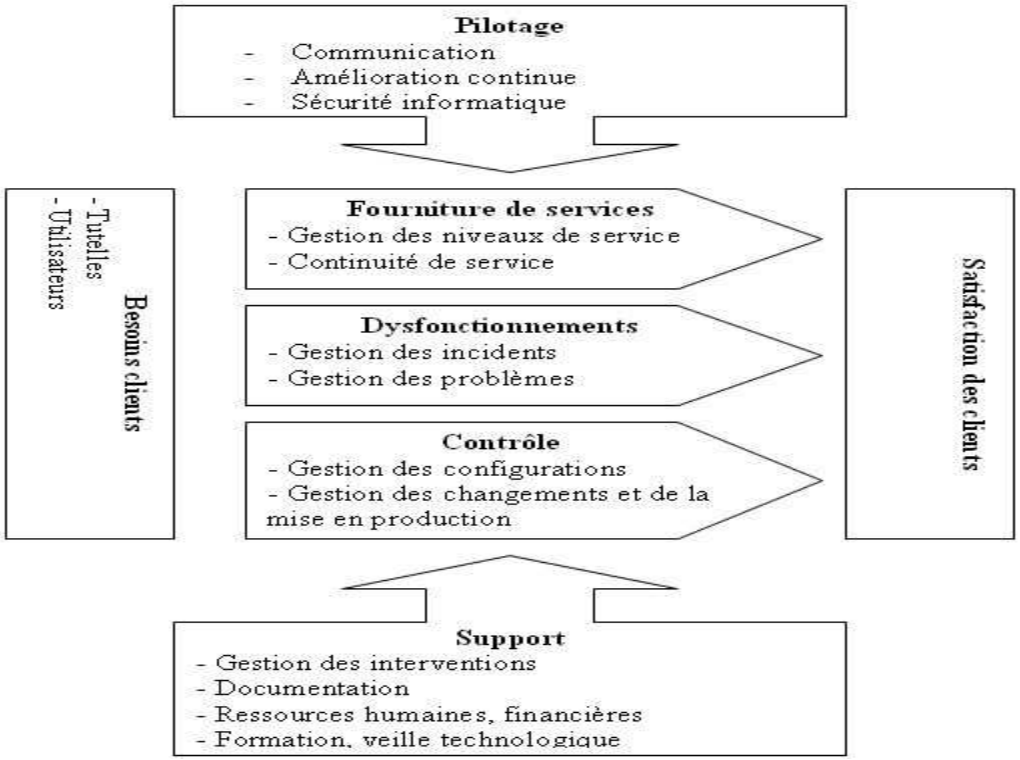
- Les bonnes pratiques d'ordre “organisationnelles” :
  - on s'inspire du modèle d'organisation découlant du standard ITIL et de la norme ISO20000-1-2 pour
  - établir les bonnes pratiques dans la fourniture de services informatiques.
- Ces référentiels itil et iso20000 :
  - fournissent un modèle pour la gestion des services informatiques et la qualité de service, et
  - introduisent un niveau d'organisation alors que seuls les aspects techniques sont traditionnellement pris en compte par les ASR..

- *Notre guide fournira en outre des pointeurs vers des fiches « techniques » décrivant des solutions logicielles ou matérielles pour prendre en charge tel ou tel processus*

GBP : fourniture de service informatique selon ITIL

- La « fourniture de services » décrit les services devant être fournis aux utilisateurs pour répondre aux besoins de l'entreprise de manière adéquate :
  - *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 comment on s'assure que le "client" a accès aux services informatiques appropriés :
  - *Le centre de service (helpdesk)*
  - *la gestion des incidents et problèmes*
  - *la gestion des changements*
  - *la gestion de la mise en production*
  - *la gestion des configurations*

Les processus de fourniture de service adaptés à un contexte de laboratoire



GBP : contenu

- Les bonnes pratiques dans la gestion de la sécurité et des contrainte réglementaires :
  - les bonnes pratiques liées à la l'application de la sécurité du SI dans l'unité, et
  - Les bonnes pratiques liées aux aspects juridiques et réglementaires *(le triptyque information – contrôle - action).*
- Les bonnes pratiques liées au profil personnel et relationnel des ASR :
  - aspects du métier qui requièrent de la méthode et capacités d'organisation personnelle (gestion du temps, agenda, planning..),
  - des qualités de communication, de compréhension et souvent de diplomatie vis a vis de nos utilisateurs.

GBP : contenu

- Les bonnes pratiques relatives à la "mise à niveau des compétences" :
  - compétences fortement évolutives dans notre métier et qui
  - nécessitent de s'intéresser à la veille technologique et à la
  - formation continue :
- comment l'ASR peut (et doit) s'adapter et évoluer dans un métier sujet à des avancées technologiques importantes.

GBP : fourniture de service informatique

- 1. Définir le périmètre d'action
  - Comme préalable à toute organisation, L'ASR doit, dans un premier temps, définir son périmètre d'action en spécifiant ses domaines d'intervention et/ou en excluant les domaines qui ne sont pas de sa responsabilité
- 2. Mettre en place une gestion des configurations
  - Ce processus s'intéresse à la gestion de l'infrastructure informatique. Cette étape nécessite d'effectuer un inventaire de l'ensemble des composants aussi bien matériels (ordinateurs, équipements réseau …) que immatériels (documentations, licences, contrats…) du service.
- 3. Définir les niveaux de service
  - La définition des niveaux de service doit permettre aux utilisateurs de connaître la nature et l'étendue du support offert par le service informatique. Chaque « niveau de service » sera associé à des objectifs réalistes visant à assurer un niveau de qualité satisfaisant à la fourniture de ce service.

GBP : fourniture de service informatique

- **1. Définir la continuité de service**
  - Associé à chaque niveau de service, l'ASR devra spécifier les exigences des utilisateurs de l'unité, en termes de continuité des services. Cet engagement établi en accord avec la Direction (et/ou une commission d'utilisateurs) sera évalué régulièrement.
- **2. Gérer les interventions**
  - Il convient de prendre en compte de manière efficace toutes les demandes d'intervention qu'il s'agisse de demandes d'intervention des utilisateurs ou de changements à apporter aux éléments du système.
- **3. 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.
- **4. Assurer les changements et la mise en production**
  - Tout changement apporté au système d'information doit être maîtrisé afin de minimiser le risque d'incident potentiel lors de sa mise en place.

... Merci de votre attention...

Questions?