

Éditorial
Quelle sécurité ?
par Philippe Pieri

_ 1

La protection du patrimoine
scientifique : une démarche
globale
par Jean-Michel Trio

_ 1

Analyse de l'environnement
numérique du laboratoire
par Magali Daujat

_ 5

Formations ISO27001
par Marc Herrmann

_ 6

La plate-forme PLUME fête
son premier anniversaire
par Jean-Luc Archimbaud

_ 8

ÉDITORIAL

Quelle sécurité ?

PHILIPPE PIERI

Délégué régional Alsace du CNRS

Dans un précédent éditorial, Jean-Marie Durand, Haut Fonctionnaire de défense et de sécurité du Ministère de l'enseignement supérieur et de la recherche, posait clairement les enjeux de la protection du patrimoine de notre organisme.

Il incitait chacune et chacun d'entre nous, acteurs de la construction de cette sécurité, à prendre fortement conscience de la « haute valeur du patrimoine du CNRS et des convoitises qu'il génère » et appelait de ses vœux « des comportements adaptés de chacun dans la perspective d'une défense en profondeur ».

Le présent numéro de « sécurité de l'information » aborde aujourd'hui plusieurs questions de fond :

- Quel besoin d'organisation ?
- Quelle méthodologie ?
- Quelles compétences à mobiliser ?

Il esquisse également les contours du management de la sécurité, qui, dans un contexte particulièrement évolutif de notre milieu de l'enseignement supérieur et de la recherche, présente plusieurs spécificités :

- L'accélération de la dématérialisation des informations (nous ne sommes toutefois en cela, pas très différents de l'évolution que vivent tous nos partenaires, qu'ils soient académiques ou industriels)
- L'optimisation de nos partenariats, notamment avec les universités, qui bénéficient d'une autonomie nouvelle ou qui l'obtiendront dans un futur proche. Ceci entraînant une réorganisation de nos services d'appui à l'activité scientifique, et la recherche d'une mutualisation de certaines compétences lorsque cela est possible. Cette évolution conduira à un partage plus clair de nos responsabilités respectives.
- La prise de conscience et l'obtention d'un équilibre entre « compétences techniques pures » (en particulier portées aujourd'hui par les ASR¹), et « compétences organisationnelles ou managériales » qui sont indispensables à chaque équipe dirigeante, en laboratoire, ou en délégation régionale.

La prise en compte des spécificités rappelées ci-dessus nous a amenés, à Strasbourg, à intégrer plusieurs démarches parallèles (PSSI, audits financiers, labellisation des plate-formes, etc.) dans un projet qualité d'ensemble dont l'aboutissement est matérialisé par les contrats de service, signés par chaque Directeur d'unité et par le Délégué régional.

L'importance et le degré de sensibilité élevé de notre patrimoine scientifique imposent une mobilisation de chacun au service de cette démarche d'amélioration continue.

« Être au niveau des meilleurs » est à ce prix !

philippe.pieri@aroba.alsace.cnrs.fr

¹ Administrateur Système & Réseau.

La protection du patrimoine scientifique : une démarche globale

Jean-Michel Trio

Adjoint du Délégué Régional Alsace du CNRS

Le patrimoine scientifique d'un laboratoire a depuis toujours été matérialisé sous forme de « papiers » : cahiers, articles, thèses, actes, etc. Passer en une seule génération de chercheurs à une forme entièrement numérique transmissible instantanément dans le monde entier constitue une véritable révolution culturelle. Facteur de progrès indéniable, cette situation crée aussi de multiples problèmes de préservation des informations, d'organisation et de partages de responsabilités entre les acteurs. En prendre conscience et mettre en place un management adapté constitue un enjeu stratégique auquel chaque laboratoire doit faire face à très court terme.

► Le Contexte

Le support du patrimoine scientifique s'est dématérialisé

Depuis peu, l'ensemble des connaissances scientifiques constituant le patrimoine d'un laboratoire est créé, modifié, transmis et sauvegardé sous forme numérique. Si le support papier reste évidemment très utilisé, l'essentiel est désormais dématérialisé sur les disques durs des stations, des portables ou des serveurs.

Mais qui s'est vraiment occupé d'organiser sérieusement ce nouvel environnement ? Chacun, chercheur, doctorant, ingénieur ou technicien, « étale » ses documents non plus sur son bureau ou sur ses étagères mais sur les gigaoctets de disques durs ou de clés USB de plus en plus nombreux et dispersés. Si on y ajoute les innombrables échanges croisés de pièces jointes enfouies dans les messageries, peut-on encore vraiment parler de « système » organisé d'informations ?

Pour ne prendre qu'un exemple courant, qui peut garantir qu'après son départ du laboratoire le travail réalisé par un doctorant est bien toujours disponible, avec tous les détails nécessaires, surtout quelques années plus tard ?

>>> suite page 2

Ne faut-il pas commencer par organiser sérieusement l'environnement numérique du laboratoire avant de pouvoir tout simplement le protéger et le conserver ? D'une part, les piratages externes sont grandement facilités par cet éparpillement des informations mais, de plus, il ne faut pas oublier que plus de 70 % des dégradations ou des pertes de données ont des causes purement internes, la plupart étant dues à cette désorganisation de fait.

Le parc informatique est pour une large part composé de produits de grande consommation

La plus grande partie des éléments constituant le parc informatique du laboratoire est maintenant en vente partout à des prix de grande consommation. Du coup, il n'est pas rare de voir des portables privés, propriétés personnelles d'un chercheur ou d'un doctorant, se mélanger avec les postes de travail du laboratoire. Garder conscience que les informations présentes sur ces postes privés font partie du patrimoine du laboratoire et doivent à ce titre rester accessibles en permanence par les personnes habilitées n'est pas forcément immédiat.

De plus, sauf pour des plateformes informatiques particulières, dédiées au calcul ou au pilotage d'expérimentation par exemple, la standardisation et la banalisation des systèmes d'exploitation et des logiciels est telle que chacun se sent maintenant capable d'administrer lui-même son poste de travail.

Pour heureuse que soit cette simplification, elle ne va pas sans une redéfinition du métier de l'administrateur système et réseaux (ASR) du laboratoire. De purement technique initialement, son rôle s'oriente maintenant davantage vers l'organisation, le management et la sécurisation des ressources informatiques.

Les moyens sont de plus en plus mutualisés

Avec leur banalisation et leur multiplication en très grand nombre, il est normal que tous ces éléments informatiques fassent de plus en plus l'objet de traitements mutualisés et pas seulement pour leur achat en volume. Avec les contraintes budgétaires, il faut chercher à optimiser les ressources en commençant par la plus rare : celle des ressources humaines !

La question est donc maintenant posée carrément : le laboratoire ne pourrait-il pas externaliser la gestion de ses moyens

informatiques en les confiant à une structure centralisée ? Et dans ces conditions, un ASR par laboratoire est-il encore indispensable ?

► Le partage des responsabilités

Plus que jamais l'organisation de la mixité et les relations de partenariat du CNRS, principalement avec l'Université, sont au cœur des débats et à la base du partage des tâches et des responsabilités. Appliqués à l'organisation de l'environnement numérique du laboratoire, trois principes peuvent être utilement rappelés :

Le mandat de gestion unique confié soit à l'Université soit au CNRS ne doit pas avoir d'incidence directe sur l'organisation du système d'information du laboratoire

En effet, c'est l'existence même d'un patrimoine scientifique propre au laboratoire et sa préservation qui sont les objectifs primordiaux de l'organisation du système d'information.

Il ne faut pas confondre la gestion des moyens informatiques, support de l'information, avec l'information elle-même : *c'est elle qui constitue le patrimoine scientifique du laboratoire*. La valeur marchande du support en lui-même est dérisoire par rapport à lui.

Dès lors, que le mandat de gestion soit confié au CNRS ou à un partenaire n'a pas d'impact direct sur l'organisation qu'il faut définir, mettre en place, surveiller et faire évoluer. En particulier, la définition des missions confiées à l'ingénieur qui en a la charge est complètement indépendante de son attachement administratif à l'un ou à l'autre.

Un élément du support informatique ne peut pas être techniquement administré à plusieurs

Cette règle de base est bien connue et fait partie de l'expérience de tout administrateur systèmes et réseaux. Par « plusieurs » il faut d'abord entendre des entités différentes, en l'occurrence soit le laboratoire soit le service centralisé en charge de l'administration des moyens mis en commun. Les méthodes de travail ne sont évidemment pas les mêmes et ne poursuivent pas les mêmes objectifs.

Mais à cet aspect s'ajoute en plus celui, plus stratégique, de la *sensibilité* de l'information. La préservation d'une information sensible est a priori antinomique avec le fait qu'elle soit présente sur un

serveur administré de façon mutualisé sauf si la Politique de Sécurité du Système d'Information (PSSI) du laboratoire encadre et contractualise strictement cette pratique.

Tous les éléments de l'environnement numérique du laboratoire doivent s'intégrer dans une organisation bien définie et faire l'objet de procédures d'usage

Cette règle de bon sens, malheureusement encore peu répandue, trouve naturellement son application lorsqu'une organisation interne est définie à la suite d'une démarche qualité adaptée.

Il faut noter que cette règle s'applique autant sur les éléments gérés en interne dans le laboratoire que sur des éléments mutualisés en relation avec un service centralisé.

Bien évidemment, la plus grande partie de ces règles ou procédures seront sensiblement les mêmes pour tous les laboratoires. Elles seront donc fort utilement établies et tenues à jour en commun grâce à un travail renforcé en réseau « métier » d'ingénieurs. Inutile en effet de redécouvrir dans chaque laboratoire la plus grande partie des mêmes « guides de bonnes pratiques ». Mais ceci n'enlève pas pour autant la nécessité d'une appropriation et d'une mise en œuvre personnalisée adaptées précisément à chacun des laboratoires.

Dans ce contexte, la Coordination Régionale de Sécurité des Systèmes d'Information (CRSSI) a un rôle déterminant à jouer pour assurer le pilotage et la coordination entre les différents organismes. Il est donc fort utile qu'elle soit ouverte à tous les acteurs concernés par la protection des patrimoines scientifiques des laboratoires de recherche.

► Les pistes d'actions proposées

Dans un tel contexte, il est nécessaire de bien se focaliser sur l'essentiel en faisant nettement la séparation entre le « bébé » que constitue le patrimoine scientifique sous sa forme dématérialisée, et « l'eau du bain » que représente la plateforme informatique courante (hormis bien sûr les constructions informatiques et les conceptions logicielles spécifiques qui font elles-mêmes partie du patrimoine). Si nous ne voulons pas risquer de « jeter le bébé avec l'eau du bain », trois actions sont à entreprendre dans chacun des laboratoires :

- **Établir précisément le périmètre du système d'information du laboratoire**

en identifiant la localisation et le traitement des informations sensibles constituant le cœur du patrimoine informationnel. Par définition, ces informations avec les ressources qui les portent ne sont pas « externalisables ».

A l'inverse, mutualiser autant que possible tout ce qui n'en fait pas partie : accès au réseau internet, WIFI, téléphonie sur IP, messagerie, serveurs web, etc. sans oublier toutefois que le laboratoire est, et doit rester, le maître d'ouvrage de ces ressources.

- **Mener une démarche qualité interne** pour organiser et rationaliser l'environnement numérique du laboratoire en préalable à la définition d'une politique de sécurité bien adaptée et réaliste.

- **Redéfinir les missions des ingénieurs informatiques dans les laboratoires.**

En effet dans de nombreux cas l'ingénieur occupant l'emploi-type « systèmes et réseaux » a vu son métier évoluer vers celui « d'architecte de système d'information ». Une formation adaptée est à mettre en place pour accompagner ou parfaire ce changement, en particulier pour tout ce qui touche à la protection du patrimoine.

Le point 1 fait l'objet de la suite de cet article. Il portera sur la description de la situation type d'un laboratoire mixte CNRS-Université en s'attachant à mettre en évidence les limites de responsabilité des différents acteurs.

Le point 2 fait l'objet de l'article de Denis Wagner plus loin dans ce journal. Cet article est basé sur l'expérience des actions pilotes menées dans le cadre de la mise en place des contrats de service dans la délégation Alsace.

Le point 3 est déjà lancé au niveau national puisque deux à trois formateurs internes par région ont suivis une formation de haut niveau dans ce domaine et sont maintenant en mesure, à leur tour, de la dispenser à leurs collègues. L'article de Marc Herrmann et de Jean-Marc Muller en fait la présentation également plus loin dans ce journal.

► **Les frontières du système d'information du laboratoire**

Une cartographie générale

Sur cette cartographie « type », et bien sûr largement non exhaustive, le demi-plan haut regroupe les éléments du système d'information (données, supports et traitements) managés et administrés en

propre par le laboratoire et le demi-plan bas ceux qui sont managés et administrés en commun par un service central, souvent attaché à une université.

L'axe horizontal permet de positionner les éléments en fonction de la sensibilité des informations traitées.

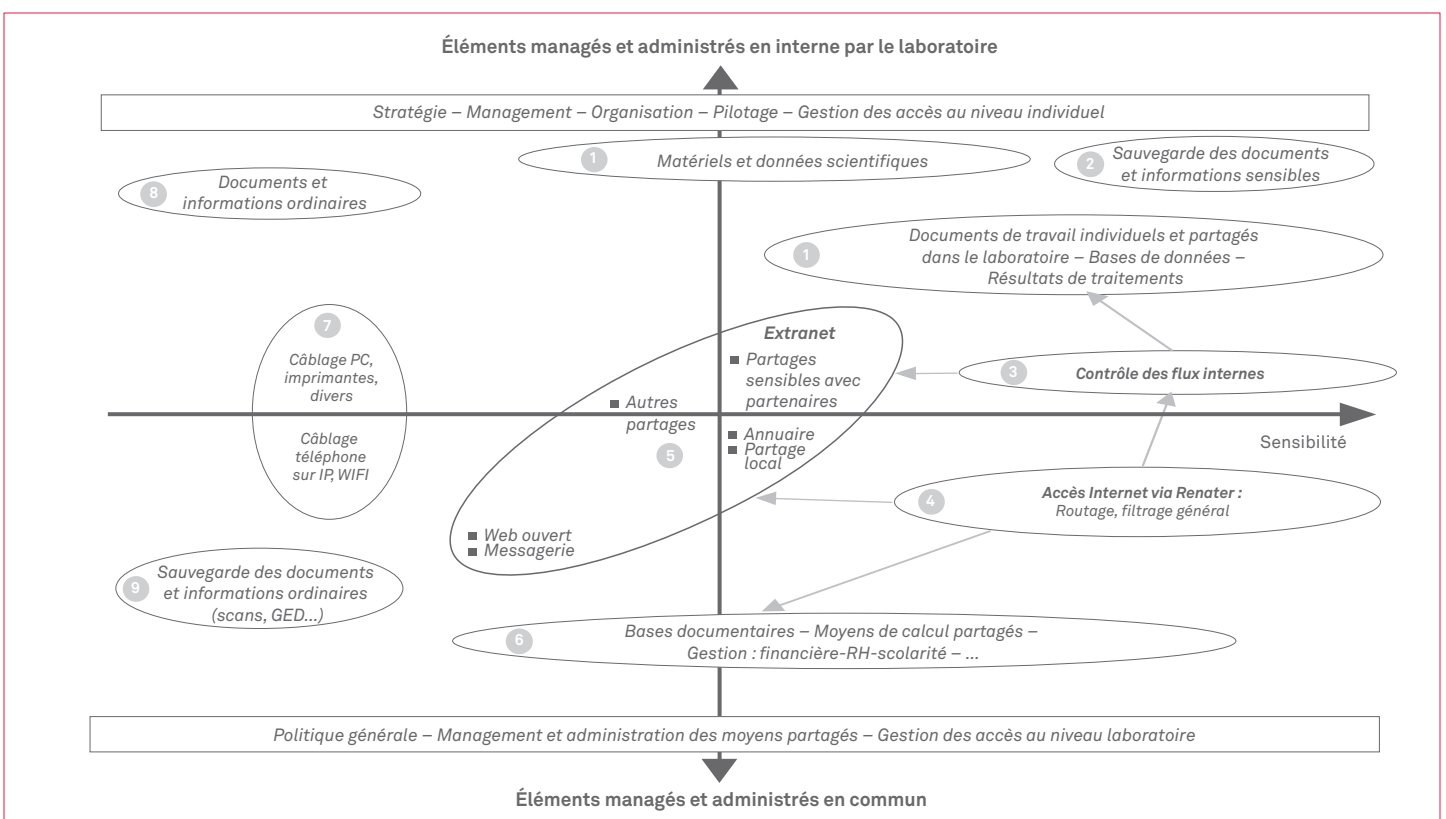
1 **Les ressources internes du laboratoire**

Par définition, ces ressources sont le cœur du système d'information du laboratoire. Il comprend à la fois les installations informatiques consacrées directement à l'activité scientifique et l'ensemble du parc interne dédié aux traitements des données sous toutes ses formes réalisés sur des postes de travail individualisés et des serveurs dédiés ou partagés dans le laboratoire.

Compte tenu des regroupements de laboratoires, il est à noter que ce parc s'étend souvent sur plusieurs bâtiments, voire même sur plusieurs campus, avec éventuellement des organismes hébergeurs différents.

Fort heureusement, la continuité ne pose maintenant plus de problème technique car elle peut aisément être assurée via des communications privées et sécurisées entre les bâtiments.

Dans tous les cas, localisation unique ou non, il est important pour l'existence même d'un système d'information cohé-



rent propre au laboratoire qu'il y ait unicité de management et d'administration et que celle-ci soit basée précisément sur l'identification de *chaque utilisateur inscrit dans un certain nombre de rôles* lui ouvrant l'accès aux ressources correspondantes. Seul le laboratoire lui-même est capable d'assurer l'organisation à ce niveau de finesse. Ceci est même critique pour les laboratoires à sensibilité élevée.

2 La sauvegarde des informations sensibles

Complément obligatoire des ressources internes cette sauvegarde a pour vocation de préserver l'intégrité de l'ensemble du patrimoine scientifique du laboratoire. A ce titre, *c'est l'élément le plus critique* de tout le système d'information du laboratoire. Il est donc nécessairement sous son contrôle direct et total. Les expériences catastrophiques malheureuses de Toulouse et Mulhouse l'ont bien montré : c'est à partir de ces sauvegardes que les laboratoires ont pu reprendre leurs travaux. La caractéristique essentielle, malheureusement pas toujours respectée, est donc que cette sauvegarde ne soit pas hébergée dans le même bâtiment que les informations qu'elle protège. Facile à réaliser en « sauvegarde croisée » quand le laboratoire occupe plusieurs bâtiments, il faudra dans le cas contraire (ou en plus) envisager l'hébergement d'un serveur du laboratoire dans un autre bâtiment du CNRS ou de l'Université. Ce serveur sera alors administré à distance par le laboratoire et fera normalement l'objet d'un chiffrement des données.

3 Le contrôle des flux internes

Les contrôles des flux entre les sous-réseaux internes du laboratoire, éventuellement étendus à plusieurs localisations, sont réalisées à l'aide d'un ou plusieurs pare-feux (firewall). C'est aussi sous leur contrôle que s'établiront les connexions distantes.

Basé sur une reconnaissance individuelle de chaque utilisateur, l'administration de ces pare-feux est sous la responsabilité directe du laboratoire.

4 L'accès internet via Renater et le routage global

Au cœur du câblage des campus et des bâtiments, cette ressource commune est la pièce maîtresse des systèmes d'information de tous les laboratoires. Son ad-

ministration, sa gestion et sa surveillance sont placées sous la responsabilité du service central au niveau régional, généralement sous la tutelle d'une université.

Véhiculant des informations de toutes natures, dont les plus sensibles, cet élément est stratégique et fait toujours l'objet de beaucoup d'attentions : surveillance des flux, redondance matérielle, règles précises d'usage, etc.

Le routage, le contrôle et le filtrage s'effectuent globalement pour l'ensemble des campus et, sauf en cas d'incidents, ces règles s'appliquent globalement au laboratoire sans descendre au niveau de l'utilisateur ou du poste.

5 La zone « extranet » du laboratoire

Par définition, cette zone semi-ouverte est le siège des échanges entre le laboratoire et tous ses partenaires au sens large. Elle couvre donc naturellement les quatre quadrants de la carte : sensible ou non, mutualisé ou en propre.

Une attention particulière doit évidemment être apportée aux d'informations sensibles échangées avec d'autres laboratoires ou co-contractants externes. Dans ce quadrant, les échanges se font sur des serveurs placés directement sous la responsabilité du laboratoire avec un contrôle d'accès et de filtrage très fin grâce à un pare-feu du laboratoire.

Par-contre, les trois autres quadrants de l'extranet peuvent faire l'objet d'une administration et d'un contrôle mutualisé.

6 Les ressources partagées au niveau établissements

Par définition, l'administration et la gestion de ces ressources est faite par le service central. Le laboratoire est en position d'utilisateur pour accéder aux bases de gestion (financière-RH-scolarité), moyens de calcul partagés, bases documentaires, etc. Selon le cas, les données peuvent elles-mêmes être sensibles au niveau des établissements, mais elles ne sont pas placées sous la responsabilité du laboratoire.

7 Le câblage informatique du laboratoire

Par câblage, il faut entendre non seulement le raccordement physique via des baies de brassage mais également les connexions logiques dans les commutateurs. A priori, l'administration du câblage est naturellement à la charge du labora-

toire qui place et déplace les éléments à son gré dans ses locaux. Mais la situation se complique quand il y a partage de locaux entre plusieurs entités dans un même bâtiment avec des baies de brassages en commun.

De toute façon, il faut aussi régler la question du câblage du téléphone sous IP et des bornes WIFI placées dans les locaux du laboratoire. Dans les deux cas, il s'agit d'une ressource partagée qui doit être administrée en commun par le service central, ce qui inclut d'office la gestion de leurs connexions physique et logique.

Les solutions seront donc à établir au cas par cas mais toujours en respectant les contraintes :

- d'administration des commutateurs par une seule entité, soit le laboratoire soit le service central,
- de réactivité pour effectuer les modifications simplement et rapidement,
- de sécurité, au moins pour les laboratoires à régime restrictif.

Dans la plupart des cas la séparation physique des flux à l'aide de commutateurs différents apportera une solution élégante et sans grands surcoûts à ce partage des responsabilités. D'autant qu'alors le choix et l'achat du matériel pourra se faire selon les habitudes de travail et les contraintes de l'un ou de l'autre.

8 Les documents et informations ordinaires

Ces documents regroupent l'ensemble des autres informations, notamment sur papier. Ils sont évidemment matériellement sous la responsabilité du laboratoire. La difficulté est qu'ils font souvent un peu trop « partie des meubles » et ne font pas toujours l'objet de l'attention qu'ils méritent pour les protéger des pertes ou des destructions. La encore, il faut assurer leur protection et leur duplication au moins sous forme virtuelle par scans systématiques.

9 Sauvegarde des documents et informations ordinaires

Ces documents, ou leurs doubles, sont à placer soit physiquement dans des locaux d'archives soit sous forme numérique sur des serveurs *hors du même bâtiment*. Un espace réservé sur des serveurs mutualisés peut fort bien convenir dans ce cas sauf s'il est plus simple et moins onéreux d'utiliser les serveurs de sauvegarde des informations sensibles en jouant sur les droits d'accès individualisés.

>>> suite page 7

Analyse de l'environnement numérique du laboratoire

Par Magali Daujat

Institut de Biologie moléculaire
des Plantes

Jennifer Jund

Délégation Alsace du CNRS

Denis Wagner

Institut de neuro-chimie

La démarche de la délégation alsace se veut de mettre en place un processus d'amélioration continue de la diminution des risques portant sur les informations numériques. Cette mission s'accompagne d'une vision claire et réaliste de l'organisation de l'environnement numérique des laboratoires. Dans un souci de globalité et d'efficacité, nous nous sommes placés dans le cadre du projet national du CNRS « Contrat de Service » pour initier ce travail avec certains laboratoires pilotes. Rappelons que les lignes directrices du contrat de service sont : service d'appui aux laboratoires, échanges privilégiés, engagement réciproque, processus d'amélioration continue...

L'approche globale proposée permet de mettre en évidence l'importance de l'organisation de l'environnement numérique pour l'amélioration générale des modes de fonctionnement du laboratoire (patrimoine scientifique, gestion financière, valorisation...).

Cet article tend à réunir non seulement les activités de sécurité, mais également de dresser un pont entre le milieu de la sécurité et celui de la qualité. La conséquence en est l'intégration progressive de la sécurité de l'information dans le champ des activités communes de l'organisation.

La Méthodologie

Les objectifs de cette méthode sont de sensibiliser les acteurs de la recherche à la protection de leur patrimoine scientifique (articles, données, thèse...), faire un état des lieux de la composante numérique du laboratoire, proposer une organisation générale de l'environnement numérique afin d'augmenter l'efficacité et la fiabilité du système d'information du laboratoire.

Phase 0 : Introduction de la démarche dans le cadre du contrat de service

La méthode est proposée au laboratoire dans le cadre de la présentation générale du projet « contrat de service ». A l'issue de cette phase, un groupe de travail commun (4-5 personnes) est constitué, regroupant des représentants choisis du laboratoire ; 1 ingénieur qualité et 1 ingénieur métier mis à disposition par la délégation.

Phase 1 : présentation de la méthodologie et sensibilisation de la direction

Présentation du projet à la direction du laboratoire : objectifs, phases, thèmes (gestion de l'information, mobilité, formation...). Résultat : cadrage du projet, choix des thèmes abordés, choix des participants...

Phase 2 : Etat des lieux et Analyse du système d'information

- Entretien avec le chargé du système d'information : organisation du système d'information, schéma directeur
- Dialogue avec les utilisateurs sur les thèmes retenus par le laboratoire : attentes, besoins, dysfonctionnements

Exemple de thème récurrent : sauvegarde du patrimoine scientifique

Résultats : Identification du périmètre de l'environnement numérique du laboratoire et des besoins des utilisateurs

Phase 3 : Synthèse

- Bilan concerté du groupe de travail laboratoire + délégation des entretiens réalisés.
- Présentation à la direction du laboratoire.
- Proposition d'un plan d'actions.
- Présentation du bilan et du plan d'action à la direction de la délégation.

Résultats : cartographie du système d'information, mise en évidence des composantes numériques sensibles et à protéger, proposition d'actions d'amélioration

Phase 4 : Validation du projet

- Validation conjointe entre les directions du laboratoire et de la délégation des actions à engager et des moyens à mettre en œuvre.
- Intégration des engagements réciproques dans le contrat de service

Résultats : plan d'actions validé et moyens alloués

Et après... Mise en œuvre des actions et amélioration

Les actions validées et planifiées sont réalisées par toutes personnes compétentes ce qui contribue à l'amélioration globale de l'organisation du laboratoire. L'analyse de l'environnement numérique de travail du laboratoire contribue à la prise de conscience de l'importance de la préservation du patrimoine scientifique et de mettre en évidence les éléments stratégiques du laboratoire.

Notre démarche est donc le lancement de la Politique de Sécurité du Système d'Information (PSSI) qui formalisera l'organisation de la protection du patrimoine scientifique en améliorant la gestion des risques. ■

Magali Daujat[aroba]alsace.cnrs.fr

jennifer.jund[aroba]alsace.cnrs.fr

denis.wagner[aroba]neurochem.u-strasbg.fr

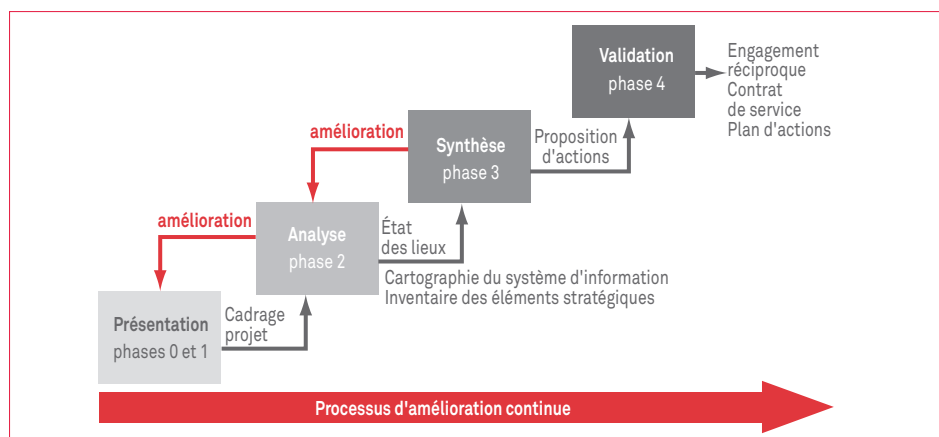


Illustration des différentes phases de la méthodologie

Formation ISO27001 : Mise en place d'un Système de Management de la Sécurité de l'Information (SMSI)

La probabilité de succès d'une opération isolée portant cachet « sécurité informatique », sous-section de la sécurité de l'information, elle-même sous-section du système d'information est bien mince, sauf à disposer d'un directeur labellisé ISO9001 et d'un ASR certifié ISO27001 à ISO27999.

Le nombre infime de laboratoires ayant déployé une PSSI en atteste ... sans parler du nombre infime de ceux qui pratique une gestion efficace des traces.

Fort de ce constat, la démarche estampillée « Sécurité du Système d'Information » s'inscrit logiquement dans un processus de management global au niveau le plus élevé du laboratoire.

Marc Herrmann
Délégation Alsace,

Jean-Marc Muller, LSIIIT,
Laboratoire des Sciences de l'Image,
de l'Informatique et de la Télédétection

► Système de management : la cible, c'est le patrimoine sensible

Un des objectifs du système de management global vise à **donner à l'équipe de direction du laboratoire les moyens d'assumer ses responsabilités et d'orchestrer son système d'information, notamment au niveau de sa sécurité.**

L'équipe de direction doit savoir où se localisent l'ensemble des actifs sensibles du laboratoire et comment accéder à l'ensemble des informations importantes. Elle doit également savoir comment sont conservés ces *éléments stratégiques* pour un usage ou une consultation ultérieurs et si les niveaux de protection de ces éléments sont acceptables eu égard aux contextes et enjeux scientifiques.

Le processus management global intègre un volet SMSI qui est lui aussi naturellement piloté par l'équipe de direction du laboratoire. Le Chargé de Sécurité du Système d'Information (CSSI) rattaché à la direction est chargé de la mise en œuvre du projet SMSI décliné en 4 étapes :

1. Référencer l'intégralité du patrimoine numérique du laboratoire.

Cette phase est réalisée lors de la démarche « analyse de l'environnement numérique du laboratoire » décrite dans l'article précédent.

2. Déterminer et classifier les points névralgiques du système d'information

Une fois les éléments stratégiques inventoriés, une *analyse de risques* permet de définir l'exposition de chaque éléments

aux diverses menaces et, au final, d'établir une liste classifiée de dangers réels ou potentiels.

3. Définir un plan d'action et les moyens associés pour obtenir un niveau de sécurité acceptable

L'établissement de cette hiérarchie des dangers permet alors de définir une suite ordonnée d'actions à entreprendre et de justifier un ensemble de moyens matériels et humains à mobiliser.

La norme ISO 27002 fixe les orientations en rassemblant 133 mesures de sécurité de type *organisationnel, technique* ou *technico-organisationnel*.

La mise en œuvre des mesures techniques relèvent de l'ASR qui peut s'appuyer sur les différentes structures d'ex-

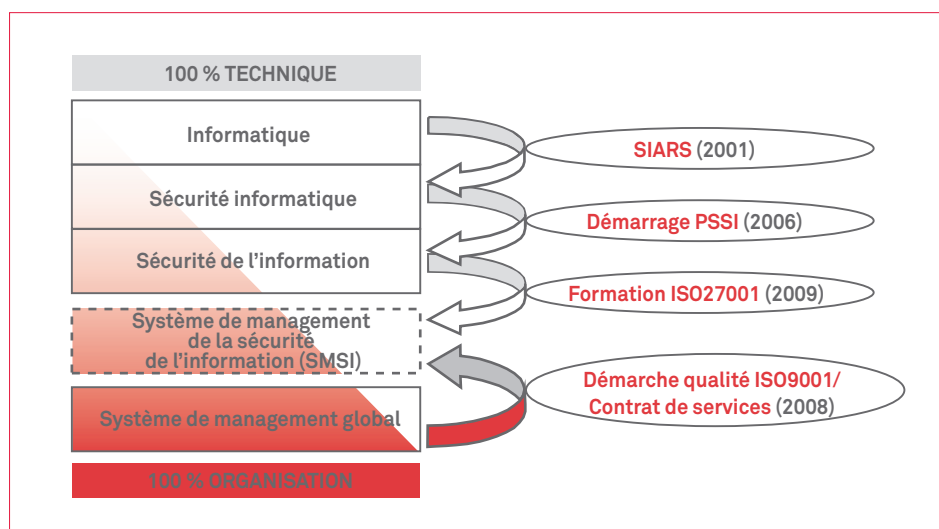
pertise technique qui demeurent des références fortes en matière de sécurité appliquée.

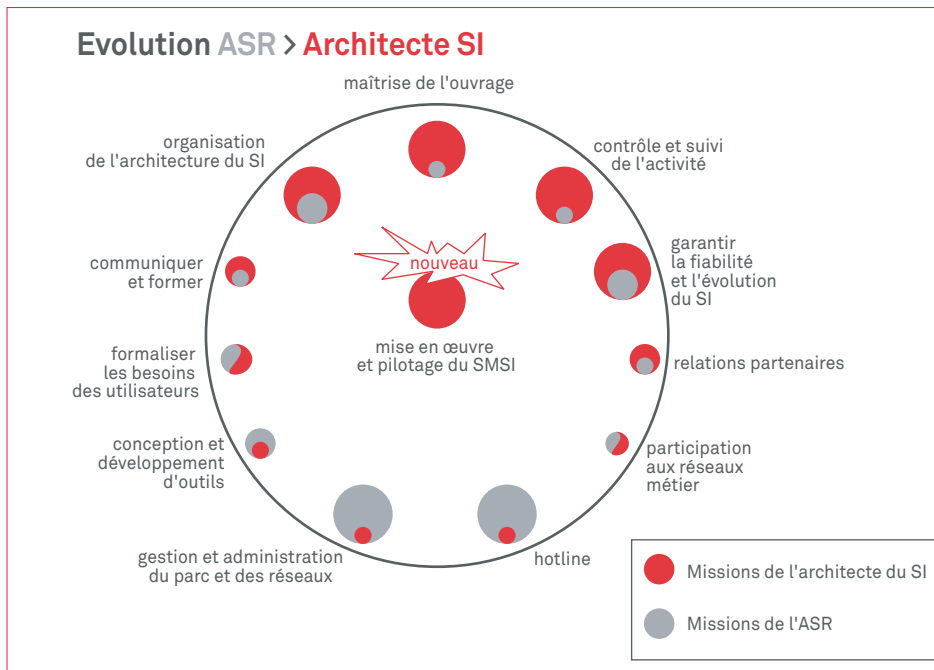
La mise en œuvre des mesures mixtes et organisationnelles se fait de concert avec la direction et concernent l'ensemble du personnel et même toute personne ayant un lien quelconque avec le système d'information du laboratoire.

La mise en œuvre globale des mesures de sécurité nécessite et exige l'association de compétences managériale ET technique.

4. Garantir la persistance du système par un mécanisme d'amélioration continue

Un système est pérenne s'il intègre régulièrement les évolutions de ses composantes. Des contrôles réguliers et ciblés ainsi que





des remontées automatiques d'informations pré-formatées permettront à l'équipe dirigeante et au CSSI de consolider le système de management par une remise en question permanente des méthodes.

► Du besoin d'organiser la technique

Historiquement, la composante sécuritaire du domaine de l'informatique puis plus globalement du système d'information était partie intégrante des missions de l'ASR, qui endossait mécaniquement la fonction de « correspondant sécurité ». Les missions de l'ASR ont évolué notamment avec la sophistication des systèmes,

la diversification des menaces et la disparition des frontières du système d'information. Cette tendance se poursuivra pour atteindre le schéma « connecté à tout, partout et tout le temps ». Dans ce contexte mouvant, les missions de l'ASR s'étendent et une nouvelle fonction sécuritaire se dessine.

La campagne SIARS (Sécurité Informatique pour les Administrateurs Réseaux et Systèmes) menée par l'UREC a placé définitivement la sécurité au cœur des préoccupations des systèmes informatiques. Le rattachement de l'informatique à l'information semble lui aussi consommé – l'in-

titulé de cette publication en est un bel exemple –, l'étendard PSSI est élevé. Reste à incorporer la PSSI dans le SMSI en suivant la norme ISO27001 et ce SMSI dans un schéma de management global au travers de la démarche qualité et des contrats de service.

► Quel profil pour le CSSI ?

Le CSSI est maître d'œuvre pour la mise en place du SMSI. En fonction de la taille et de l'exposition du laboratoire, le CSSI peut avoir plusieurs profils différents.

- Spécialiste des systèmes d'information à la base, l'ASR « classique » peut endosser les missions du CSSI mais doit associer de nouvelles compétences managériales pour évoluer vers l'emploi type *architecte des systèmes d'information*. (voir schéma ci-dessous)

L'ASR pourra acquérir ces compétences en suivant les formations ISO27001 organisées au niveau national par le FSD et dispensés en région par des experts certifiés *Responsible d'implémentation ISO27001*

- Un membre de l'équipe de direction peut également devenir CSSI à condition qu'il complète cette même formation ISO27001 par une bonne connaissance des différents concepts d'architectures des systèmes d'information et des notions de base sur les technologies des systèmes informatiques et des réseaux.
- Enfin, dernière possibilité, en fonction de l'importance et la structure d'une unité, le CSSI peut être secondé dans ces fonctions par d'autres personnes de l'unité, la ventilation des tâches devant alors être précisée. ■

marc.herrmann[aroba]alsace.cnrs. fr
muller[aroba]lsiit.u-strasbg. fr

Marc Herrmann, Jean-Marc Muller et Denis Wagner sont membres de la coordination Régionale SSI en tant qu'experts certifiés ISO27001 (LSTI) et Jennifer Jund est ingénieur qualité à la délégation Alsace du CNRS.

>>> suite de la page 4

► Les deux écueils les plus redoutables

Au final, les deux écueils à éviter absolument sont bien connus mais ils n'en demeurent pas moins redoutables :

Ne rien faire

« Mon micro marche, j'ai accès à internet et à ma messagerie, donc tout va bien. Occupons-nous de questions plus importantes ».

Sous la pression des impératifs de qualité, imposés notamment par les

contrats, les directeurs de laboratoires prennent la mesure du problème et veulent agir. Nous commençons donc enfin à nous éloigner de ce premier écueil.

Oublier le bébé en ne s'occupant que de l'eau du bain

Cet écueil est malheureusement encore devant nous : « L'informatique n'est pas mon métier, je sous-traite tout mon matériel à un service central et je retourne m'occuper de mes missions ».

Certes indispensable pour la maîtrise des coûts en ce qui concerne la *mise en œuvre des moyens*, cette mutualisation a ses limites. Elle ne diminue en rien la responsabilité du laboratoire en matière d'organisation et de maîtrise de la qualité dans tous ses domaines d'excellence.

Et tous ces domaines s'appuient d'une manière ou d'une autre sur une *utilisation intelligente et maîtrisée* de l'informatique. ■

Jean-michel.trio[aroba]alsace.cnrs. fr

La plate-forme **PLUME** fête son premier anniversaire

Jean-Luc Archimbaud,

directeur du projet PLUME

CNRS/UREC

► **État de l'art**

Il y a un an, le 5 novembre 2007, la plate-forme PLUME (<http://www.projet-plume.org>) était ouverte. Ce projet, initialisé par le CNRS à travers l'UREC, Unité Réseaux du CNRS, a rapidement été soutenu par un certain nombre d'acteurs (Centre de calcul de l'IN2P3, LAAS, INIST, INSA Lyon, CNAM, RENATER...). Destinée à Promouvoir les Logiciels Utiles Maîtrisés et Economiques dans la communauté de l'Enseignement Supérieur et de la Recherche (CNRS, universités et autres EPST), son objectif est triple :

- 1°) Mutualiser les compétences en logiciels, la plupart libres, dans la communauté Enseignement Supérieur et Recherche en présentant des fiches descriptives des logiciels utilisés en production dans les laboratoires et universités, fiches rédigées par des personnels de ces entités.
- 2°) Promouvoir les développements de la communauté en référençant les logiciels développés dans les laboratoires de recherche et les services associés.
- 3°) Favoriser les échanges et améliorer l'expertise par la création d'une communauté d'ingénieurs et de chercheurs compétents en logiciel, à la fois des concepteurs et des utilisateurs avertis.

Cette plate-forme publique présente aujourd'hui 174 logiciels validés, 12 logiciels à valider, 7 logiciels en test, 54 développements « Enseignement supérieur / Recherche » (sauf exceptions des logiciels libres et gratuits), 61 ressources (articles, cours...) avec 285 contributeurs et 661 membres. L'ensemble des documents est indexé pour permettre des recherches thématiques, par métier... La consultation du serveur a doublé en 6 mois pour atteindre plus de 990 000 accès en janvier. En parallèle,

différents projets connexes (apprentissage en ligne, école thématique...) sont lancés.

L'année écoulée a été principalement consacrée à mettre en production les bases techniques et organisationnelles de la plate-forme. Les mois qui arrivent seront destinés à :

- 1°) enrichir la base des descriptions de logiciels et autres documents associés, en particulier sur les développements internes avec un objectif de valorisation au sens large (projet RELIER avec une partie du site en anglais),
- 2°) organiser des actions de formation pour permettre une meilleure utilisation de ces logiciels
- 3°) aider la communauté des développeurs par des formations, documents de référence, groupes d'échanges régionaux ou thématiques,
- 4°) stabiliser et renforcer l'organisation qui repose sur quelques personnes,
- 5°) mettre en place et organiser de nouveaux soutiens et partenariats à ce projet et à cette plate-forme.

L'objectif général est de rendre un service global d'information sur les logiciels, la plupart libres, d'un côté utilisés et de l'autre produits par l'Enseignement Supérieur et la Recherche.

► **La sécurité des systèmes d'information dans PLUME**

Un binôme de responsables thématiques se met en place et devrait être officialisé dans les prochaines semaines. Mais déjà un mot-clé « domaine informatique=sécurité » existe. Vous pouvez consulter tous les documents à ce sujet à partir de la page : <http://www.projet-plume.org/fr/fiches-documents> ou directement avec le lien : <http://www.projet-plume.org/fr/secureite>

Vous pouvez vous abonner au flux RSS [secureite](http://www.projet-plume.org/fr/secureite) qui annonce tous les documents

PLUME traitant de la sécurité à partir de la page : <http://www.projet-plume.org/fr/info-rss> ou directement avec l'URL :

http://www.projet-plume.org/fr/objets_securite_par_date/feed

N'hésitez pas à décrire les logiciels sécurité que vous utilisez et appréciez dans PLUME. Pour contribuer : <http://www.projet-plume.org/fr/contributions>

► **En conclusion**

N'hésitez pas à consulter le site, les membres de la communauté Enseignement Supérieur et Recherche sont invités à contribuer. Pour plus d'informations, consultez le site <http://www.projet-plume.org> ■

Jean-Luc.Archimbaud[aroba]urec.cnrs.fr

SÉCURITÉ DE L'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :

Joseph Illand
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris cedex 16
Tél. : 01 44 96 41 88
Courriel : joseph.illand[aroba]cnrs-dir.fr
<http://www.sg.cnrs.fr/fsd>

Rédacteur en chef :

Robert Longeon
Chargé de mission SSI du CNRS
Courriel : robert.longeon[aroba]cnrs-dir.fr

Impression : Bialec, Nancy (France) - D.L. n° 70568

ISSN 1967-7219

La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine.