Introduction à la sécurité des systèmes d'information

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ DE LA SANTÉ

Guide
pour les directeurs
d'établissement de santé

novembre 2013

Direction générale de l'offre de soins

L'offre de soins doit se déployer autour des patients, dans une logique de parcours – de santé, de soins, de vie – de décloisonnements entre les différents acteurs, de coordination et de complémentarité

A ce titre, les systèmes d'informations sont des outils de partage et d'échanges incontournables au bénéfice des patients, des professionnels et du système de santé. Il est donc crucial de garantir leur sécurité, leur disponibilité et leur confidentialité pour maintenir la confiance des patients dans le système de santé et celle des professionnels dans les outils qu'ils utilisent au quotidien

La politique de sécurité ne se limite pas à la protection contre la perte, l'indisponibilité ou la divulgation de données médicales personnelles ou administratives, elle permet de créer un espace de confiance entre les professionnels et les patients et elle est un levier essentiel de l'amélioration de la qualité des soins. Il est donc de la responsabilité du management des établissements de santé (Directeur, Directeur des soins, Directeur des Ressources Humaines, présidents des conférences ou commissions médicales des établissements de santé) de la promouvoir.

S'appuyant sur le retour d'expérience de deux projets régionaux, qui regroupent chacun une trentaine d'établissements, le présent guide éclaire la problématique de la sécurité, en précise les enjeux et présente aux décideurs, les étapes de la mise en place d'une démarche.

Bonne Lecture

Jean Debeaupuis.

Comment lire ce guide ?

Ce guide pratique vise à apporter un éclairage sur les enjeux de la sécurité du système d'information dans un établissement de santé et à exposer aux décideurs quelles sont les bases de la mise en place d'une démarche de sécurité. Il est principalement destiné aux équipes de direction des établissements publics et privés (Directeur, Directeur des soins, Directeur des Ressources Humaines, DAF, …), aux Présidents de CME et aux chefs de pôle ; mais il peut être lu par l'ensemble des Professionnels de Santé et des cadres de ces établissements.

CONTEXTE

Ce guide s'appuie principalement sur le retour d'expérience de deux projets régionaux, dans le Nord Pas de Calais et dans le Limousin. Ces projets, actuellement en cours, regroupent chacun une trentaine d'établissements. Ils visent à faire élaborer une politique de sécurité par chaque structure, mettre en place une organisation pérenne pour la sécurité du système d'information (SI) et conduire différents projets de sécurité (utilisation de la carte de professionnel de santé (carte CPS) pour l'accès au SI, plan de continuité d'activités, …).

Ce guide fait partie de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), référentiel qui est en cours de rédaction (publication fin 2013), et en est un élément constitutif. La PGSSI-S exprime des exigences de sécurité et des principes de mise en œuvre ; elle fixe des objectifs globaux, pérennes ; elle est aussi constituée d'un document qui rappelle le cadre et les obligations juridiques ainsi que de référentiels techniques sur les différents thèmes de la sécurité des systèmes d'information. La PGSSI-S est destinée à l'ensemble des personnes qui utilisent des données de santé (organismes de recherche, médecins libéraux, établissements de santé, etc.) ; elle vise tous les modes d'exercice (exercice libéral, laboratoire, établissements de santé, etc.). Ce guide permet d'aborder plus facilement les autres documents de la PGSSI-S, sans être un préalable.

CONTENU DU GUIDE PRATIQUE – QUE TROUVE-T-ON DANS LES FICHES ?

Ce guide est composé de 10 fiches pratiques. Elles expliquent la démarche de sécurité SI et contiennent des recommandations sur des points clés que sont notamment la réalisation d'un diagnostic et le pilotage de la démarche avec le soutien de la Direction.

- **La Fiche N°1 « Les enjeux de la sécurité de l'information pour l'établissement de santé »** rappelle, pour l'établissement, les enjeux et le contexte vis-à-vis des nouvelles technologies de l'information et de la communication.
- **La Fiche N°2 « Maîtriser la sécurité du Système d'Information (SI) – Comment ? »** reprend les éléments significatifs et incontournables de chaque thème abordé dans le guide. Elle donne les objectifs d'une démarche de sécurité du système d'information (SI) avec les principes permettant de maîtriser sa mise en place et les actions prioritaires pour initier la démarche.
- **La Fiche N°3 « Définition de la sécurité du Système d'Information dans les établissements de santé »** présente le fondement d'une démarche sécurité ainsi que les projets majeurs liés à cette démarche.
- **La Fiche N°4 « La Direction acteur important de la démarche sécurité »** précise les différents points où l'action de la Direction est nécessaire.
- **La Fiche N°5 « Pré-requis : un diagnostic et une gouvernance sécurité »** indique par quoi commencer et donne des repères pour mettre en place l'organisation de la démarche sécurité.

- **La Fiche N°6 « La sécurité avant d'autres projets : le bon arbitrage »** propose aussi de commencer par des actions « pépites » relativement faciles à mettre en place, qui permettent de constituer un socle de sécurité et d'initier la démarche.
- **Fiche N°7 « Les facteurs clés de succès de la démarche »** décrit les retours d'expérience d'organisation de démarches réussies au sein des établissements.
- **Fiche N°8 « La communication : un levier essentiel »** rappelle l'importance de la communication et les messages principaux dans une démarche sécurité.
- **Fiche N°9 « La documentation sécurité : un minimum est nécessaire »** décrit les principales briques documentaires.
- **Fiche N°10 « Les coûts de la sécurité »** donne des pistes pour une évaluation budgétaire des couts de la sécurité.

COMMENT LIRE LE GUIDE PRATIQUE

L'ordre de lecture des fiches n'est pas imposé ; Chaque fiche peut être lue sans avoir nécessairement pris connaissance des fiches précédentes.

EN CONCLUSION

Le guide constitue pour la Direction un document de sensibilisation sur les questions de sécurité des systèmes d'information ; il s'inscrit dans le corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S). Avec ce guide pratique, la Direction de l'établissement possède les clés pour comprendre les enjeux de la sécurité du SI et pour initier une démarche pérenne avec l'appui de ses équipes.

Sommaire

Fiche n°1 : Les enjeux de la sécurité de l'information pour l'établissement de santé

1 - L'EVOLUTION DES PRATIQUES ET DES TECHNOLOGIES

L'usage progressif du **Dossier Patient Informatisé** (DPI) dans les établissements montre que les soins s'appuient de plus en plus sur le système d'information (SI).

La standardisation des technologies fait que la barrière séparant les **équipements biomédicaux** du reste du réseau informatique tend à disparaître. Le pilotage de ces équipements et les données traitées se trouvent donc dépendants de la sécurité globale du Système d'Information (SI).

L'utilisation des technologies de l'information améliore la qualité des soins, les conditions de travail… mais elle est aussi porteuse de nouveaux risques et de nouvelles contraintes.

Ainsi, la mise en place du DPI doit être accompagnée d'une garantie de disponibilité 24h/24 et 7j/7, et d'authenticité des informations s'y trouvant. Un dysfonctionnement du SI entrainant un mélange de résultats de biologie peut avoir un impact fort sur une prise en charge d'un patient.

Une nouvelle dimension du SI pour les établissements de petite taille - *CH de Néris-les-Bains* : *Le déploiement du DPI s'est accompagné d'une augmentation importante du nombre de machines «en 2 à 3 ans, nous sommes passé de 15 à 60 postes avec aujourd'hui 3 serveurs. On sentait arriver les problèmes sans pouvoir les qualifier. On était aveugle mais on commençait à être conscient de notre vulnérabilité».*

Les logiciels antivirus, les mots de passe et les sauvegardes informatiques des données sont indispensables pour éviter des incidents, **mais les mesures strictement techniques ne suffisent pas à répondre à l'enjeu.**

2 - LE LIEN ENTRE INCIDENTS DE SECURITE ET QUALITE DE L'OFFRE DE SOINS

L'informatisation de la prise en charge du patient rend celle-ci vulnérable à tout incident impactant le système d'information.

Prenons un exemple tiré de fait réel : lorsqu'un virus paralyse les applications utilisées dans la gestion des urgences, cet incident peut engendrer une désorganisation des interventions et des accès à l'information relative à l'état de santé du patient.

Ce n'est pas l'utilisation des systèmes d'information au sein des établissements de santé qui est en cause ici, mais les liens possibles entre un incident informatique et son impact sur la sécurité du patient et la qualité de sa prise en charge.

3 - LES CONSEQUENCES DES INCIDENTS DE SECURITE

Les pertes **d'intégrité**, de **disponibilité**, de **confidentialité** et **de traçabilité** de l'information médicale, peuvent engendrer des conséquences cliniques importantes, ainsi que des répercussions possibles sur la notoriété de l'établissement. En voici quelques exemples :

- **Une indisponibilité** des données de santé à un moment crucial (intervention chirurgicale, administration de médicaments, consultation,…) peut entraîner la répétition d'un acte, une imprécision, des retards ou des erreurs dans les diagnostics ou les soins, et se traduire par une perte de chance pour le patient par méconnaissance de son contexte et de ses historiques médicaux ;

- **Un défaut d'intégrité** de la donnée de santé, comme l'altération accidentelle ou illégitime d'un dossier de santé ou du paramétrage d'un équipement biomédical, est susceptible d'entraîner des erreurs médicales, voire un préjudice vital envers le patient.

- **Un défaut de confidentialité** d'un document de santé, comme la divulgation à la famille, aux services d'une société d'assurance ou d'un employeur d'un résultat positif de dépistage de tumeur maligne, pourrait porter préjudice au patient, puis par voie de conséquence, au professionnel de santé et/ou au responsable de la perte de confidentialité.

- **L'absence de preuve sur l'auteur** d'un document médical (ex. ordonnance) dont la lecture aboutit à une erreur médicale, ne permet pas d'imputer l'erreur à la personne réellement en cause et de trouver la source des erreurs.

Les traces permettent de dégager sa responsabilité – *CH de Seclin* : *La DSI a été accusée d'avoir fait fuiter des primes de service. L'absence de traces informatiques n'a pas permis de dégager sa responsabilité et de démontrer que la négligence provenait d'un utilisateur.*

Ces conséquences seront considérées comme des manquements graves aux obligations éthiques et aux engagements de l'établissement.

4 - LES MENACES QUI PESENT SUR LE SYSTEME D'INFORMATION

Les menaces pesant sur l'intégrité, la disponibilité ou la confidentialité des informations sont souvent liées à des **erreurs humaines** (du fait de la négligence ou de l'ignorance).

Dans un établissement de la région Nord Pas-de -Calais : *Suite à une mauvaise gestion des droits administrateur, un utilisateur a supprimé par erreur une branche d'un Active Directory (annuaire informatique des utilisateurs). Cet incident a entrainé une impossibilité de se connecter au SI pour une grande partie de la population de l'établissement de santé pendant 48h.*

Les **erreurs d'implémentation des systèmes** sont aussi à l'origine d'incidents ; enfin, la **malveillance externe** est bien réelle et souvent négligée.

Dans un établissement d'un groupe de cliniques *: Suite au licenciement difficile d'un infirmier, ce dernier, via sa connaissance des identifiants et mots de passe de médecins, a procédé à de nombreuses prescriptions sans fondement obligeant le corps médical à vérifier chaque prescription faite au cours des dernières semaines »*

Voici quelques exemples d'incidents pouvant affecter un établissement de santé :

- **Négligence du personnel dans la protection des données par méconnaissance des risques.** A cause de cette ignorance du risque, des données médicales se sont retrouvées indexées sur les moteurs de recherche internet début 2013 dans un hôpital. Le premier fait est le recours à un hébergeur externe non agréé, par méconnaissance des risques du stockage des données médicales à l'extérieur de l'établissement ; il n'a pas été tenu compte du cadre réglementaire, du « décret hébergeurs » (Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel). Le second fait est la négligence de l'hébergeur qui dans la conception de son système de stockage a rendu possible que les dossiers médicaux soient visibles par les moteurs de recherche. (Lire l'article sur *Le Monde* du 19 mars 2013).

Dans un établissement de la région Nord Pas-de -Calais : *L'absence de connaissance des risques conduit à des imprudences. Ainsi suite à des raisons historiques dans un établissement, un pont de visioconférence été ouvert sur Internet en clair. Les visioconférences qui servaient à des conversations d'ordre médical, étaient accessibles à tout le monde depuis Internet.*

- **Introduction d'un virus dans le système d'information.** Une grande partie des incidents de sécurité informatique impliquent la propagation de virus. Des moyens techniques peuvent en limiter la propagation (anti-virus) mais le facteur humain ou la conception des systèmes peuvent faciliter leur diffusion. En mars 2009, le virus « Conficker » a infecté plusieurs millions d'ordinateurs et on comptait, parmi les cibles, un grand nombre d'établissements de santé en France. L'utilisation de clés USB (non sécurisées) par les médecins ou la mauvaise sécurisation de certains appareils connectés au réseau (appareils biomédicaux, ordinateurs personnels, etc.) sont autant de points de fragilité du système d'information qui sont exploités par les virus.

« ActuSoins a mis le doigt sur des failles et des maladresses du personnel de santé qui permettent à tout un chacun de prendre connaissance, [via Internet,] de données médicales confidentielles. » (Lire l'article sur le site ActuSoins, http://www.actusoins.com/12771/des-donnees-medicales-confidentielles-accessibles-sur-le-web.html.

« […] la contamination par un ver informatique génère des coûts dus au non-fonctionnement de système et au travail supplémentaire nécessaire des informaticiens et des techniciens. Un coût qui peut s'avérer particulièrement élevé. » (Lire l'article sur TICsante.com, http://www.ticsante.com/print_story.php?story=495)

- **Vols externes.** Le vol de données par des personnes extérieures peut se faire par une entrée physique dans l'hôpital mais également à distance *via* Internet. Des failles de sécurité dans les applications ou le réseau peuvent permettre à un hacker d'accéder aux données stockées sur les serveurs d'un établissement, de les subtiliser et, dans certains cas, de perturber le fonctionnement du SI.

« Le Federal Bureau of Investigation (FBI) a ouvert une enquête suite à une demande de rançon reçue par les autorités de l'État de Virginie. Celle-ci s'élève à 10 millions de dollars et concerne plus de 8 millions de dossiers médicaux.

Ces derniers ont été détournés par un ou des hackers sur le site web du service du gouvernement de Virginie collectant des informations pour pister l'usage abusif d'ordonnances de médicaments. Ces dossiers contiennent quelque 35 millions de prescriptions, couplées aux numéros de Sécurité sociale et à l'adresse des patients, que le pirate se dit prêt à vendre si la rançon ne lui est pas versée pour qu'il restitue ces données à la Virginie. Le problème est d'autant plus ennuyeux que le site Internet ne disposerait pas d'une sauvegarde de ces informations, selon le hacker.[…] » (article sur droit-medical.com - avril 2009)

D'autres menaces existent : le **vol interne**, les dommages matériels intentionnels ou non, la **défaillance de connexion Internet ;** il faut aussi indiquer **le bug d'un logiciel, la panne d'un matériel informatique ou du réseau**, qui peuvent conduire à un arrêt complet du système, si les mesures de sécurité sont inexistantes ou incomplètes.

5 - LA SECURITE POUR MAITRISER LE COUT DES INCIDENTS

La sécurité est souvent perçue comme génératrice de coûts sans que le retour sur investissement ne soit directement perceptible. Or, c'est avec le coût de la non qualité des soins qu'il faut comparer le coût des investissements nécessaires pour se protéger des incidents de sécurité.

Le rapport entre coût de la sécurité et l'impact de ne rien faire est parfois disproportionné *: « Le logiciel anti-virus n'a pas été installé sur les postes de travail. Une trentaine de postes de travail sont infectés et inutilisables tant qu'ils n'ont pas été désinfectés. Ainsi, les utilisateurs de ces postes ne peuvent plus travailler jusqu'à leur rétablissement. Quelques dizaines d'euros auraient pu éviter de devoir assumer pour l'établissement l'équivalent d'une demi-journée d'absence pour les personnels concernés. »*

Il faut regarder la sécurité comme « le coût de ne pas faire » ; c'est-à-dire, évaluer l'ordre de grandeur de l'impact financier (et opérationnel, en particulier sur la qualité des soins) d'un risque qui se réaliserait. Il est alors nécessaire d'analyser les risques qui pèsent sur le SI de l'établissement et d'évaluer leurs impacts.

Fiche n°2 : Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Une démarche de sécurité du système d'Information (SI) dans un établissement ne peut exister sans l'impulsion de la Direction pour légitimer sa mise en œuvre.

1 - LES OBJECTIFS DE LA SECURITE DU SYSTEME D'INFORMATION (SI)

Trois grands objectifs sont fixés à la démarche de sécurité du SI.

1.1 - Objectif 1 : Garantir l'intégrité de l'information en évitant toute altération ou perte de données

Réduire le risque de perte ou d'altération des données du SI est l'un des objectifs principaux.

Pour atteindre cet objectif, l'une des actions prioritaires doit porter sur **la mise en œuvre d'un plan de sauvegarde des données du SI.** L'expérience montre que ce plan n'est jamais efficace à moins d'être testé régulièrement (sauvegardes incomplètes, restauration impossible, absence de procédures de reprise des données non sauvegardées, etc.) ; ces tests sont **exécutés avec la collaboration des utilisateurs du SI** de l'établissement.

Pour garantir la qualité de l'information, les praticiens des établissements interrogés expriment le besoin de pouvoir établir les responsabilités en cas d'anomalie ou d'altération sur des données de santé. Pour répondre à ces besoins, une deuxième action consiste à **activer dans les applications du SI, autant que possible, des fonctions de génération de traces associée aux opérations réalisées sur les données**; les traces obtenues doivent être conservées au moins 3 mois pour pouvoir être exploitées en cas de recherche de la cause d'une anomalie.

Un incident touchant l'intégrité des données, vécu dans un établissement de la région Nord Pas-de-Calais

« Un matin, nous avons découvert des anomalies dans certains numéros de sécurité sociale de notre base de patients. La remise en état des 40.000 dossiers a nécessité l'intervention de deux personnes à temps plein pendant une semaine.»

1.2 - Objectif 2 : S'assurer de la continuité des services en cas de défaut grave de l'informatique

Elaborer un plan de continuité d'activité pour s'assurer qu'en toutes circonstances, les activités vitales de l'établissement ne seront pas arrêtées. En cas d'arrêt du SI, ce plan prévoit des **procédures palliatives qui devront être suivies par les utilisateurs**. Des cas ont montré qu'un arrêt pouvait entraîner, s'il n'est pas correctement géré, des pertes de chances pour des patients, une perte d'image et des pertes d'activité pour l'établissement.

Les situations suivantes ont été vécues dans des établissements consultés pour la rédaction de ce guide : le logiciel ou le serveur hébergeant le DPI ne fonctionne plus ; l'alimentation électrique est coupée ; un pourcentage important des postes informatiques sont infectés par un virus et ne fonctionnent plus.
Tous admettent qu'une **préparation adaptée avant ces incidents** mettant en œuvre des moyens techniques, des procédures, de l'organisation, aurait permis d'éviter des situations parfois critiques.

Un arrêt de plusieurs jours du SI - *Syndicat Inter-hospitalier du Limousin* : *« Suite à la tempête de 1999, l'informatique dans certains établissements a été arrêté pendant plusieurs jours par manque d'électricité »*

1.3 - Objectif 3 : Garantir la confidentialité des données à caractère personnel

Un établissement de santé traite des données à caractère personnel qualifiées de sensibles par la loi « informatique et libertés » (article 8 de la loi).

Au-delà de la contrainte règlementaire, et à côté du préjudice potentiellement grave subi par les patients dont les données médicales ont été divulguées, force est de constater que ces incidents –la diffusion massive de données médicales- font de plus en plus souvent l'objet d'une médiatisation et atteignent alors l'image de l'établissement.

Aussi, l'établissement doit mettre en pratique toutes les **mesures nécessaires pour garantir la confidentialité des données. Ces mesures ne sont pas que seulement techniques.** Elles nécessitent, pour être efficaces, d'adapter des processus métiers et de faire adhérer les professionnels de santé à des pratiques réflexes.

Le travail d'**un Correspondant Informatique et Libertés (CIL),** bénéficiant des qualifications requises pour exercer ses missions, est un fort contributeur à la démarche visant à garantir la confidentialité des données. Il existe en effet une forte convergence entre le CIL et le responsable de la

sécurité du SI. Bien qu'ayant des périmètres différents, les deux fonctions cumulent des actions communes en matière de sécurité, de confidentialité et de sensibilisation. Elles sont parfois assurées par la même personne.

2 - REPONDRE AUX EXIGENCES REGLEMENTAIRES ET DE CERTIFICATION

L'établissement doit assurer sa conformité par rapport aux multiples exigences règlementaires et répondre aux critères de certification. Plusieurs intègrent la sécurité des systèmes d'information (certification HAS, certification des comptes, etc.). Ils s'appuient pour la plupart sur un socle normatif commun (famille des normes ISO 27000, et voir fiche 5 l'encadré sur « les référentiels de sécurité ») . **La démarche sécurité permet de répondre à ces obligations.**

En cas de négligence notoire, la responsabilité du dirigeant de l'établissement est engagée. C'est le cas notamment en matière de protection des données à caractère personnel, où la responsabilité est de nature pénale. Ces exigences sont détaillées dans **le document juridique de la Politique Générale de Sécurité des Systèmes d'Information de Santé** (PGSSI-S) (document disponible sur le site de l'ASIP Santé, avec les autres documents de la PGSSI-S).

3 - VALIDER QUE LA DEMARCHE VISE LES OBJECTIFS RECHERCHES

La Direction doit vérifier que la démarche est ciblée et cohérente avec les besoins prioritaires de l'établissement en sécurité.

La Direction doit porter une attention particulière à ce qu'une **trajectoire réaliste d'amélioration de la sécurité soit définie, afin de ne pas décourager les parties prenantes.**

(cf. *Fiches 4 et 5*).

4 - METTRE EN PLACE UNE ORGANISATION LEGITIME, CAPABLE D'ANIMER LA DEMARCHE

Dans le cadre d'une démarche sécurité, il faut mettre en place, le plus rapidement possible, une organisation de sécurité, identifiant à minima :

- **Un responsable de la démarche sécurité** à la fois reconnu et disposant d'une connaissance transverse des activités de l'établissement. Il a besoin de maîtriser ses processus et son organisation. Il peut s'appuyer sur d'autres compétences notamment pour les aspects liés à l'architecture du SI, la sécurité et les aspects juridiques et contractuels. Le responsable qualité de l'établissement peut être la bonne personne pour cette mission. **Il agit en tant que maître d'ouvrage sécurité**.
- **Un correspondant opérationnel de la sécurité** ayant une bonne connaissance de l'informatique de l'établissement et des aspects techniques de sécurité. Il a en charge de mettre en œuvre et de maintenir les mesures de sécurité pour ce qui relève de l'informatique.

Remarque : *le responsable de la démarche sécurité peut être le correspondant sécurité. Dans ce cas, la personne doit réunir à la fois des compétences techniques informatiques, et des capacités à conduire des projets transverses dans un établissement.*

- **Une instance de pilotage** (dédiée ou non) se réunissant périodiquement et dans laquelle seront évoqués les risques et les mesures opérationnelles de sécurité. Cette instance doit réunir une représentation aussi complète que possible des services de l'établissement (DRH, Services Généraux, Informatique, services de soins, services logistiques)

(Cf. Fiche 5.)

5 - INITIER UNE DEMARCHE D'AMELIORATION CONTINUE

La démarche sécurité est un processus d'amélioration continue **à l'instar de la qualité des soins**. Il faut donc pérenniser la démarche, ce qui passe par :

- **L'organisation d'un état des lieux périodique** permettant de réaliser un nouveau diagnostic, d'identifier les écarts restant à combler et de réactualiser un plan d'actions prioritaires.
- **La définition de paliers de réalisation** des actions pour une atteinte progressive des objectifs.

Ces actions nécessitent bien entendu des moyens. Ainsi, une bonne pratique pour les établissements, quelle que soit leur taille, est de trouver une ligne budgétaire dédiée, reconduite chaque année.

6 - INFORMER ET SENSIBILISER

Les objectifs de sécurité prioritaires doivent être connus de tous et partagés. Chacun doit connaitre les risques existants, la finalité des contraintes mises en place, et les bénéfices attendus pour l'établissement et la pratique des soins.

Il est aussi nécessaire d'initier un programme de sensibilisation à la sécurité des systèmes d'information, puisque ce sont souvent les erreurs humaines des utilisateurs dans l'établissement qui sont à l'origine des incidents, du fait de la négligence ou de l'ignorance des risques.

(Cf. Fiche 8)

7 - AIDES EXTERIEURES

ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information - http://www.ssi.gouv.fr/

L'agence assure la mission d'autorité nationale en matière de *sécurité des systèmes d'information*. A ce titre, elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Elle a notamment pour mission de jouer un rôle de conseil et de soutien aux organismes. C'est pourquoi elle publie plusieurs guides qui constituent des bonnes pratiques

qui peuvent aider les établissements dans leur démarche sécurité :

- Des recommandations d'ordre technique sur les nouvelles technologies ou une démarche en cas d'incident http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/

- Des outils pour aider à construire à construire une politique de sécurité du système d'information (PSSI) http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/pssi-guide-d-elaboration-de-politiques-de-securite-des-systemes-d-information.html

ASIP Santé – Agence des Système d'Information Partagés de Santé

Chargée d'un développement pérenne des systèmes d'information dans le secteur de la santé, l'ASIP Santé s'attache à produire et mettre en œuvre, en collaboration avec les acteurs professionnels et industriels, des référentiels qui sécurisent l'échange, le stockage et le partage des données de santé.

Cnil

Dans ses missions, la Commission Nationale de l'Informatique et des Libertés conseille et renseigne les organismes qui envisagent de mettre en œuvre des fichiers informatiques. Par son service d'orientation et de renseignements, elle apporte une réponse rapide aux questions les plus fréquemment posées par les professionnels :

- Des fiches pratiques concernant la protection des données de santé (modèle de clauses pour la sous-traitance, les impératifs en matière de sécurité, http://www.cnil.fr/dossiers/sante/
- Un guide dédié aux professionnels de santé http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/professionnels_de_sante/
- Un catalogue de mesures pour aider à traiter les risques sur les libertés et la vie privée http://www.cnil.fr/fileadmin/documents/Guides_pratiques

Ministère de la santé

- **La Politique Ministérielle de Sécurité des Systèmes d'Information** s'applique à tout établissement public placé sous l'autorité du Ministère. Elle fixe les responsabilités du directeur des établissements, en tant qu'Autorité Qualifiée de Sécurité des Systèmes d'Information (AQSSI) et fournit une liste de règles obligatoires ou recommandées avec leurs déclinaisons opérationnelles.
- **La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).** Elle contient des référentiels pour aider notamment les établissements à intégrer la sécurité au SI. (Pour plus d'information, voir le site de l'ASIP santé http://esante.gouv.fr/pgssi-s/presentation)
- **Dans le cadre du programme « hôpital numérique »**, le Ministère de la Santé a défini des indicateurs de sécurité en « pré-requis » pour répondre aux enjeux de l'informatisation de la production de soins dans les établissements de santé.

La Haute Autorité de Santé

La HAS certifie les établissements de santé, elle accrédite les praticiens de certaines disciplines médicales sur la base du volontariat. Elle participe également à l'amélioration de la qualité de l'information médicale sur internet et dans la presse.

- La HAS a établi des critères de **certification dont une partie** porte sur la sécurité de l'information

Regroupements – mutualisation

La mutualisation des expertises entre plusieurs établissements, la mise en commun d'actions semblables peuvent apporter une aide. Des initiatives régionales portées par l'Ars ou des GCS régionaux sur la e-santé peuvent faciliter cette dynamique. (Il faut aussi signaler le rôle des Syndicats Interhospitaliers, des groupes de cliniques, des groupements d'achats tels que UniHA).

Ces regroupements peuvent représenter une aide :

- Des apports importants pour la démarche de sécurité (retours d'expérience, conseils, cahier des charges, etc.).

- Des apports de compétences, notamment une expertise en sécurité des Systèmes d'Information.

- Une capitalisation des connaissances et des réalisations.

.

Fiche n°3 : Définition de la sécurité du Système d'Information dans les établissements de santé

La sécurité permet de créer un espace numérique de confiance favorable à la dématérialisation, au partage et à l'échange de données de santé. Elle ne se limite pas à protéger la confidentialité des données, ni à lutter contre des virus informatiques.

La sécurité :

- **contribue à la qualité de la prise en charge des patients dans le respect de leurs droits.**
- **garantit notamment la confidentialité, la traçabilité et la pérennité des données numériques de santé à caractère personnel.**
- **offre aux professionnels de santé une « sécurité juridique » lors de l'utilisation du système d'information.**

1 - LA SECURITE DU SYSTEME D'INFORMATION

Le système d'information (SI) ne se réduit pas à l'informatique ; il regroupe l'ensemble des moyens humains, techniques et organisationnels visant à assurer le traitement, le stockage et l'échange d'informations nécessaires aux activités de l'établissement.

La finalité de la sécurité est de lutter contre les risques auxquels est exposé le SI, qui ont pour origine des défauts de conception, de développement, d'implémentation ou d'usage du SI.

Les actions de sécurité doivent agir à plusieurs niveaux :

- en protégeant le SI pour éviter que des situations risquées comme des tentatives d'intrusion ne se produisent, ce sont les actions de maîtrise des risques (par exemple : fermer les portes de locaux hébergeant le ou les serveurs, généraliser une politique efficace de contrôle des accès aux applications, limiter les droits administrateurs sur les serveurs informatiques, etc.).
- en détectant qu'un incident se produit pour réagir au plus vite et limiter sa propagation ; c'est la surveillance, la vigilance et les tests de sécurité (par exemple : disposer des détecteurs incendies, mettre en place des fiches réflexes pour remontée les incidents, activer les dispositifs de traces, et surveiller ces journaux, mettre en place des moyens d'alerte…).
- en limitant les impacts potentiels du risque s'il se produit (par exemple : disposer de sauvegardes des données et tester les procédures de restauration, avoir des procédures dégradées, de secours, de reprise, de continuité pour faire face à une panne majeure du SI, …).

2 -LES NOTIONS FONDAMENTALES DE LA SECURITE (DICP, DISPONIBILITE, INTEGRITE, CONFIDENTIALITE, PREUVE)

La sécurité regroupe 4 notions fondamentales : la disponibilité (D), l'intégrité (I), la confidentialité (C) et la preuve (P).

2.1 - La disponibilité (D) : un niveau contextualisé selon l'usage du SI (financier, médical, …).

La disponibilité des SI permet de garantir en permanence la communication et l'échange des données de prise en charge des patients, sans défaut y compris pendant les heures non ouvrées.

La disponibilité des SI qui aident à la production des soins doit être au centre des préoccupations sécuritaires des établissements.

Une panne entraîne l'arrêt du DPI – *Etablissement de la région du Limousin* « La panne d'un serveur dont le contrat de maintenance est arrivé à échéance, entraine l'arrêt du DPI. Plus aucun dossier patient n'est accessible »

Un virus bloque la production – *Etablissement de la région du Limousin* « Un virus non détecté par le logiciel anti-virus se propage, rendant inutilisables les postes de travail jusqu'à l'intervention d'un technicien spécialisé »

2.2 - L'intégrité (I) : une fiabilité maximale des données de santé et des données financières.

L'intégrité est l'objectif d'exactitude et de fiabilité des données et des traitements. Les SI doivent garantir que les informations sont identiques et inaltérables dans le temps et l'espace et certifier leur exhaustivité, leur validité et leur cohérence. En ce sens, la sécurité du SI contribue aux actions d'identito-vigilance.

Une défaillance provoque des erreurs des dysfonctionnements – *Etablissement de la région Nord Pas de Calais*

« Une mise à jour de l'application DPI (Dossier Patient Informatisé) a provoqué une modification de tous les numéros d'identification des patients, ayant failli entraîner une erreur de prescription médicamenteuse. »

« Des éléments de calcul ont été involontairement modifiés et cela a provoqué des erreurs de paie massives »

L'objectif d'intégrité est fondamental pour les données médicales ou financières.

2.3 - La confidentialité (C) : un accès modulable aux données de santé.

La confidentialité permet de réserver l'accès aux données aux seules personnes autorisées. Les données confidentielles sont les suivantes :

- Les informations protégées par le secret médical,
- Les informations privées des collaborateurs,
- Les informations de toute autre nature soumises à une obligation légale ou règlementaire de confidentialité (marchés publics par exemple),
- Les informations stratégiques dont la divulgation interne ou externe peut nuire à la réputation ou au fonctionnement de l'établissement.

Des exigences légales, notamment celles du décret confidentialité, fixent un cadre dans le traitement des données médicales à caractère personnel.

Des cas divers de divulgation – *Région Nord Pas de Calais*

« Des personnels accèdent aux dossiers médicaux de leur collègue »
« Des personnes extérieures pénètrent dans des bureaux et consultent des dossiers patients »
« L'assistante a laissé par inadvertance des documents de direction sur l'imprimante »
« Un prestataire informatique intervient dans l'établissement et fait la copie de tous les DPI de l'établissement pour disposer de données de test »

2.4 - La preuve (P) : la conservation de traces à valeur de preuve

La preuve permet l'investigation en cas de dysfonctionnement et d'incidents. Les SI doivent pouvoir fournir la preuve d'un évènement donné et permettre la vérification du bon déroulement des traitements informatiques réalisés par les applications. Les mécanismes généralement employés sont la génération de traces informatiques et un système d'imputabilité qui permet d'associer une action à son auteur.

Absence de preuve – *Région Nord Pas de Calais*

«Une modification illégitime d'un dossier RH a été détectée. Aucun élément ne permet d'identifier l'auteur»

3 - LA SECURITE UNE DEMARCHE ITERATIVE, FAITE DE PLUSIEURS PROJETS

La sécurité s'inscrit dans une **démarche d'amélioration continue, à l'instar de ce qui est fait dans la démarche qualité.**

Une trajectoire est définie, faite de **différents projets dont les plus complexes** sont :

- Le plan de sauvegarde des données.
- Les droits et les devoirs des utilisateurs.
- La sécurisation de l'infrastructure et de son exploitation.
- La gestion des identités et des accès au SI.
- Le plan de continuité et de reprise d'activité.

3.1 - Le plan de sauvegarde des données

Ce projet est un des plus critiques car il vise à restaurer les données détruites lors d'une panne en utilisant les données périodiquement sauvegardées sur un support externe. Des moyens (techniques, organisationnels) existent déjà dans l'établissement ; le projet consiste d'abord à s'assurer que ces moyens correspondent aux besoins des utilisateurs, et si nécessaire effectuer les évolutions. Des tests de restauration des données doivent être faits pour s'assurer que les moyens mis en place sont opérationnels.

3.2 - Les droits et devoirs des utilisateurs

Le facteur humain joue un rôle essentiel dans la sécurité. **Les utilisateurs doivent comprendre leurs droits et devoirs relatifs à l'usage du système d'information** et être sensibilisés aux bons réflexes (ne pas divulguer ses mots de passe, ne pas stocker ou échanger des données hors du cadre prévu, prévenir en cas d'incident, …). Les droits et devoirs des utilisateurs doivent être formalisés dans une charte d'utilisation du SI. Cette charte doit être annexée au Réglement Intérieur de l'établissement. *(cf fiches 5 et 9).*

3.3 – La Sécurisation de l'infrastructure et de son exploitation

Ce projet vise à sécuriser les éléments informatiques (poste de travail, serveurs informatiques, bases de données, bornes wifi, infrastructure réseau de l'établissement, etc.) en appliquant les bonnes pratiques issues de l'état de l'art. La première étape est de rendre redondants certains équipements matériels pour assurer, via des mécanismes de résilience, la disponibilité du système d'information en cas de panne de ces équipements.

Pour mener à bien un tel projet, une assistance extérieure est généralement nécessaire car il nécessite des compétences techniques parfois pointues.

Une compétence de sécurité est nécessaire – *Groupe Vitalia :* *« Un piège est de croire que la sécurité est quelque chose de facile. Pour mener des actions de sécurité, il est nécessaire d'avoir des compétences avérées en la matière. Aussi, deux situations doivent être corrigées :*

- *Celle où aucune sécurité n'est mise en place (exemple avéré : « le raccordement du réseau de l'établissement à une livebox sans cloisonnement ni sécurité »).*

- *Celle où une personne férue d'informatique mais non experte met en œuvre une sécurité excessive et non adaptée (exemple avéré : « mise en œuvre d'un pare-feu par service, soit la présence de 17 pare-feu pour un établissement »). »*

3.4 – La Sécurité physique des locaux

La sécurisation des accès aux locaux et aux salles hébergeant le matériel informatique permet de contrôler les personnes ayant accès physiquement aux machines ainsi qu'aux documents sensibles. Le risque de vol de poste de travail ou de support est principalement visé.

Un accès restreint aux seules personnes habilitées permet de limiter les éventuels accidents ou actes de malveillance pouvant survenir sur le système d'information.

3.5 - La gestion des identités et des accès

Le décret confidentialité du 15 mai 2007 précise l'ensemble des dispositions pour contrôler l'accès aux informations médicales nominatives. Ces obligations s'étendent à toute information à caractère personnel au titre de la loi informatique et libertés.

Dans ce contexte, comment créer un nouvel utilisateur ? Quels droits sur les applications informatiques lui donner ? Comment gérer les départs et mutations ? Comment remettre des comptes informatiques aux bons utilisateurs ? etc.

La gestion des identités et des accès au SI consiste :

- D'abord, à associer des droits d'accès (des comptes d'accès) aux personnes physiquement présentes dans l'établissement.

- Puis, à donner aux utilisateurs des moyens adaptés pour les protéger afin d'éviter une usurpation d'identité (par exemple, une carte de professionnel de santé, carte CPS).

- Enfin, à attribuer, à chaque utilisateur, les habilitations nécessaires pour utiliser les différentes applications du SI.

Ce projet implique fortement la DRH de l'établissement.

« Beaucoup d'établissement ne savent pas combien de comptes d'accès existent dans leur annuaire principal donnant accès à leurs applications ? »

3.6 – Le Plan de reprise et de continuité d'activité (PRA et PCA)

Le projet vise à mettre en place tous les dispositifs techniques, organisationnels et humains qui garantissent le maintien des activités vitales de l'établissement en cas d'incident temporaire perturbant ou arrêtant la production informatique. Le projet consiste à :

- Mettre des moyens pour redémarrer au plus vite l'informatique.

- Trouver les dispositifs qui permettront, sans informatique, de réaliser temporairement les activités selon un mode dégradé.

Les objectifs visés par le plan sont repris dans les indicateurs du programme «hôpital numérique».

Ce projet implique l'ensemble des représentants des services de l'établissement.

Un décalage des numéros de SS - *Etablissement de la région Nord Pas de Calais :* *« Nous avons découvert un jour un décalage dans tous les numéros de sécurité sociale de notre base de patients. La remise en état a nécessité l'intervention de deux personnes à temps plein pendant une semaine »*

Fiche n°4 : la Direction acteur important de la démarche sécurité

1 - Les roles de la Direction dans la demarche

Les rôles principaux de la Direction sont :

- **de valider les priorités de l'établissement** en matière de sécurité (Cf. *Fiche 5*).

C'est au Directeur de l'établissement que revient la décision d'arbitrage **entre l'acceptation d'une prise de risques et les actions à mener** visant à les éviter.

- **de désigner les acteurs clés et mettre en place une organisation** pour conduire la démarche sécurité du SI.

La responsabilité de la mise en œuvre du plan sécurité du SI NE peut être totalement déléguée aux informaticiens.

- **de communiquer** auprès de tous sur l'enjeu et les bénéfices de la démarche.
- **d'apporter un soutien actif et les ressources nécessaires** aux responsables des actions prises pour renforcer la sécurité.
- **de contrôler et de suivre dans le temps l'atteinte des objectifs.**

2 - Un « soutien » obligatoire de la Direction pour une demarche reussie

C'est le principal facteur clé de succès. La Direction doit être promoteur, doit soutenir la démarche et en rappeler, si nécessaire, les enjeux. Il faut transformer l'image de sécurité vue comme une contrainte sans apport sur la qualité et la sécurité des soins. Seule la Direction peut soutenir ce message de la sécurité créatrice de confiance sur le Système d'Information.

La sécurité est l'affaire de tous les utilisateurs. Ceux-ci doivent respecter les règles d'usage du Système d'Information, même si bien souvent ces règles sont vues comme une contrainte sans intérêt opérationnel. Pour accepter cette contrainte, il faut communiquer vers les utilisateurs et les convaincre des enjeux sous-jacents.

L'expérience dans la région du Limousin montre le rôle central de la Direction *: « La sécurité n'est ni transparente pour l'utilisateur, ni sans contrainte. La sensibilisation des utilisateurs ne suffit pas. Il est nécessaire d'imposer des règles. Seule la direction aura la légitimité indispensable pour éviter le sentiment d'une nouvelle lubie du service informatique. »*

Le soutien de la Direction, est d'autant plus important que les chantiers les plus complexes ont un **impact sur l'organisation de l'établissement et les aspects opérationnels des services**. C'est le cas, par exemple, de la gestion des identités et des accès des utilisateurs au système d'information ou de la mise en place d'un plan de continuité d'activité (en cas de panne grave du système d'information).

L'implication de la Direction est fondamental - *CH La Bassée :* *« L'implication de la Direction a été un facteur clé de la réussite de notre démarche sécurité et de sa pérennité »*

3 - Les actions a lancer par la Direction

3.1 - Désigner un pilote

Le pilote du projet global « sécurité du système d'information » aura la responsabilité d'organiser la mise en œuvre des actions sécurité et de contrôler l'efficacité des actions.

Ce pilote doit, de préférence, être rattaché à la Direction de l'établissement pour que son action soit légitime. (Cf. Fiche 5)

3.2 - Demander la réalisation d'un diagnostic

L'objectif du diagnostic est d'identifier les principaux points de faiblesse du système d'information dans l'établissement (cf. *Fiche 5*). Ce diagnostic doit être réalisé par rapport aux risques opérationnels, aux vulnérabilités intrinsèques des établissements, aux textes juridiques et réglementaires et enfin aux menaces vraisemblables auxquelles l'établissement peut être confronté.

L'état des lieux une étape nécessaire - *CHG de Cornil :* *« Ce qui a manqué, c'est de ne pas avoir commencé par un état des lieux pour savoir où en est l'établissement et identifier les priorités »*

3.3 - Valider les objectifs de sécurité

Des objectifs de sécurité pour les applications du SI doivent être formalisés par les utilisateurs.

3.4 - Valider une feuille de route et communiquer

Afin d'atteindre les objectifs de sécurité, des actions sont à conduire, qu'il faut hiérarchiser et planifier. La Direction fait les arbitrages nécessaires, s'assure que les moyens (humains, budgétaires) sont disponibles et que la trajectoire retenue est réaliste. Elle supervise ensuite la réalisation du plan d'actions.

4 - LES REGLES D'USAGE DU SYSTEME D'INFORMATION – LA CHARTE D'UTILISATION

Des règles doivent être suivies par les utilisateurs du système d'information pour en sécuriser l'usage. La difficulté réside dans la confusion que peut faire un utilisateur entre l'usage privé et l'usage professionnel de l'informatique. Dans un contexte professionnel, les objectifs de sécurité sont forts et nécessairement plus contraignants.

Selon la grande majorité des Responsable de la Sécurité des Systèmes d'Information, la plus grande menace à laquelle ils ont à faire face est l'usage inapproprié ou négligent du SI par ses utilisateurs.

Les règles fixant le cadre d'utilisation du SI sont en générales décrites dans une **« charte d'utilisation ».** Cette charte doit être **annexée au Règlement Intérieur** pour qu'elle soit opposable aux salariés. (La consultation des instances, CE, CHSCT, CME s'impose alors ainsi qu'une présentation de la charte au directoire et au conseil de surveillance). (Cf. *Fiche 9*).

5 - LES PERSONNES A ASSOCIER DE FAÇON PRIORITAIRE A LA DEMARCHE

La Direction de l'établissement peut impliquer plusieurs acteurs dans la démarche sécurité du SI en précisant leurs rôles et responsabilités. Généralement, doivent être impliqués :

- **Les services généraux** pour les aspects de sécurité physique d'accès aux locaux et de sécurisation des équipements et fluides (énergie, climatisation, incendie, Télécom).

- **Le service informatique,** est le garant de la mise en œuvre du plan d'action relevant de la sécurité informatique. Quelle que soit sa taille, c'est un interlocuteur important et incontournable en raison de sa connaissance du SI et de ses compétences techniques.

- **S'il a été nommé, le correspondant informatique et libertés (CIL)** pour l'identification des traitements sensibles et les moyens transverses de protection des données.

- **Le responsable des risques et/ou le responsable qualité et sécurité des soins**, qui, en raison de ses activités, possède une vision transverse des risques de l'établissement et permet d'intégrer la sécurité SI dans une gestion globale et coordonnées des risques.
  Remarque : il peut être chargé du pilotage de la démarche sécurité SI (Cf. Fiche 5).

L'importance de la définition des responsabilités – Groupe Vitalia : *« Deux établissements similaires déployant le DPI. Dans le premier, 4 personnes se partagent la responsabilité de l'opération ; Dans le second, 1 chef de projet est désigné. Suite à un problème sur le logiciel utilisé, dans le premier établissement, personne ne réagit. 6 mois après, survenance de gros problèmes logiciels entrainant la défiance des médecins et l'échec du déploiement. Dans l'autre cas, le problème a pu être traité immédiatement.»*

Fiche n°5 : Pré-requis : un diagnostic et une gouvernance sécurité

Comment mettre en place la démarche ; à qui déléguer le rôle de responsable ?

1 - Etablir un pre-diagnostic sans etre expert : les 10 questions a se poser

« Tout va bien. L'ensemble du système d'information fonctionne ». Cette affirmation revient souvent lorsque la question d'un budget sécurité est à arbitrer par la Direction au détriment d'autres budgets jugés plus essentiels pour l'établissement. **Voici une dizaine de questions simples qui permettent de faire rapidement un premier bilan sur la maturité de sécurité atteinte**.

1. Est-il possible de savoir combien d'heures ou de jours au total, le système d'information a été indisponible cette année? Mesurez-vous et surveillez-vous cet indicateur ?
2. Existe-t-il une politique de sécurité qui reflète la situation existante (document à jour) ? Les éventuels écarts par rapport à l'existant, l'appréciation de leurs conséquences potentielles sont-ils connus de la Direction ?
3. Le nombre de comptes d'accès nominatifs aux applications informatiques déclarés dans l'annuaire du SI est-il supérieur au nombre de personnes physiques accédant au système d'information ? Avez-vous encore des comptes génériques pour l'accès au SI ?

De très nombreux comptes inutiles - *Région du Limousin* « Le Syndicat Inter-hospitalier constate régulièrement l'existence dans les SI d'accès dédiés à des anciens personnels et qui n'ont été ni supprimés et sont encore actifs. Dans un établissement, le SIL a compté plus de 700 comptes actifs alors que l'établissement ne comporte que 300 personnes physiques».

4. Les droits d'accès au DPI permettent-ils de garantir que seules les personnes autorisées ont la possibilité de modifier des données ?
5. Des données vitales seraient-elles perdues en cas d'incendie ou d'inondation dans un local technique hébergeant des serveurs ? Le temps qu'il faudrait pour rétablir le système informatique est-il connu ?
6. Quelle est l'ancienneté des serveurs ? La maintenance est-elle assurée ? Les systèmes sur ces serveurs sont-ils très régulièrement mis à jour ?
7. Les procédures de restauration des sauvegardes de données ont-elles déjà été testées ?
8. Les données RH concernant les informations sur les personnels de l'établissement font-elles l'objet d'une protection particulière ?
9. Est-il possible que dans certaines circonstances, un visiteur puisse accéder sans difficulté à un poste de travail ?
10. Dans le cas où un dossier médical de l'un de vos personnels aurait été consulté de manière illégitime, le service informatique serait-il en mesure de fournir des éléments pour investiguer ?

2 - Faire un diagnostic d'expert et cibler l'essentiel

L'objectif du diagnostic est de fournir des indications sur les améliorations urgentes requises par rapport aux obligations règlementaires et aux manquements les plus préjudiciables. Le résultat doit permettre de présenter à la Direction la liste des risques les plus forts qui pèsent sur les activités de l'établissement et un plan des actions nécessaires pour les réduire.

Un diagnostic erroné- *Région du Limousin* *« Les principaux échecs de ces analyses est d'utiliser un questionnaire non adapté au contexte d'établissement ou de répondre sans posséder la compétence nécessaire pour appréhender dans leur ensemble les éléments à contrôler »*

Ce type de diagnostic nécessite des compétences en matière de sécurité et une connaissance approfondie du Système d'Information tant sur le plan fonctionnel que technique.

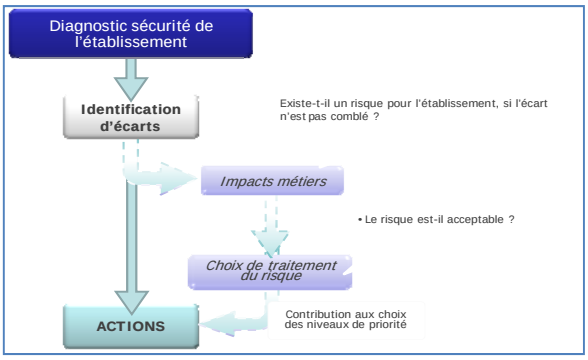
Il est fortement conseillé de faire appel à des professionnels de la sécurité qui réaliseront une prestation en collaboration avec un représentant des différentes directions de l'établissement.

Les bénéfices d'une assistance externe pour établir un diagnostic - *CH de Neris-les-bains*

« L'assistance extérieure crédibilise la démarche et ses résultats. Elle a été pour nous indispensable pour produire un plan d'action qui donne un cadre légitime pour le projet d'amélioration globale».

3 - DEMARCHE D'ANALYSE DE RISQUE

Le schéma ci-dessous présente les différentes étapes d'une démarche d'identification des risques sur la base d'un diagnostic de l'établissement.



Cette démarche est comparable à celle que l'on retrouve pour une analyse de risques sur la qualité des soins.

Elle n'a de spécifique que les domaines de compétences liés à la sécurité du Système d'Information. Il s'agit d'identifier les enjeux métier, de faire un état des lieux, d'en déduire les risques principaux pesant sur le SI (cartographie des risques) et d'en déduire un plan de traitement des risques.

4 - ELABORATION DU PLAN D'ACTIONS SECURITE

Le diagnostic (qui est l'analyse des écarts par rapport à un référentiel de règles et de bonnes pratiques) permet d'élaborer un plan d'actions pour améliorer la sécurité.

Les actions sont évaluées pour pouvoir effectuer le bon arbitrage. Les indicateurs généralement utilisés pour chaque action sont :

- Niveau de couverture des risques.
- Coûts de mise en œuvre et de maintien.
- Dépendance des actions entre elles.
- Durée de mise en œuvre.
- Difficultés de mise en œuvre.
- Compétences nécessaires et induites.
- Priorité.
- Désignation des rôles et des responsabilités.

La liste des actions est ordonnée et chaque action est positionnée dans le temps (Cf. *Fiche 6*).

Il est courant de rencontrer des plans d'action prévoyant, sur les premiers mois, une charge importante.

Les référentiels de sécurité

Un référentiel de sécurité est un catalogue de règles et bonnes pratiques sécuritaires, reconnues par la communauté des experts de sécurité.

Les référentiels de sécurité sont utilisés en appui pour réaliser le diagnostic (mesurer l'écart vis-à-vis des bonnes pratiques) et pour sélectionner les actions à mettre en place.

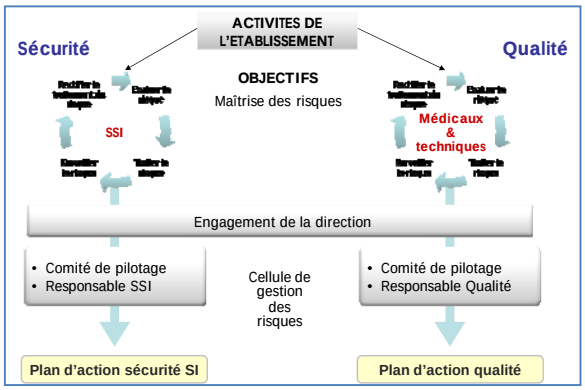
A l'heure de l'écriture de ce document il n'existe pas de référentiel de sécurité de portée obligatoire. ***Il est prévu que la Politique Générale de Sécurité des Systèmes d'Information de santé, PGSSI-S, contienne un référentiel de sécurité adapté au contexte des établissements de santé,*** *qui regroupe les différentes exigences applicables.*

Les référentiels sont nombreux mais tous s'appuient sur des principes homogènes décrits au travers de normes internationales ISO. ***La norme internationale ISO 27002 regroupe les bonnes pratiques de sécurité.*** *Sa structure est reprise dans la plupart des référentiels (par exemple, la Politique Ministérielle pour la Sécurité des Systèmes d'Information du ministère de la santé).*

- ***L'ANSSI : L'Agence Nationale de Sécurité des Systèmes d'information*** *publie un guide d'hygiène informatique. Il n'est pas spécifique au domaine de la santé, et vise l'ensemble des acteurs économiques ; il regroupe en 40 règles de sécurité les « fondamentaux » en matière de sécurité et propose une grille de suivi des actions à mener. L'Agence publie également des recommandations techniques précises sur des thématiques diverses (Wifi, le guide d'externalisation, etc.).*
- ***L'ASIP Santé*** *: Le guide fourni par l'ASIP Santé pour constituer un dossier d'hébergement contient un référentiel (P6) d'exigences obligatoires dans le cas de l'hébergement de données de santé pour le compte d'un tiers.*
- ***La Commission Nationale de l'Informatique et des Libertés (CNIL)*** *: Elle propose un catalogue de bonnes pratiques dont l'objet est de proposer des mesures de sécurité visant à protéger la vie privée des personnes.*
- ***La certification HAS et le programme "Hôpital Numérique"*** *contiennent un ensemble d'indicateurs relatifs à la sécurité des systèmes d'information dans un établissement de santé. Mais ceux-ci ne sont pas suffisants pour aborder toutes les problématiques de sécurité.*

5 - LA DEMARCHE QUALITE ET LA DEMARCHE SECURITE : DEUX DEMARCHES SIMILAIRES

Il ressort des expériences recueillies auprès des établissements du Nord Pas de Calais que **la démarche qualité et sécurité des soins et la démarche sécurité du SI présentent des ressemblances** : Cf. la figure ci-dessous.



En effet, les circuits d'identification des risques métiers impliquent les mêmes acteurs dans l'établissement.

> Les établissements interrogés indiquent qu'une gouvernance unique de gestion des risques est réalisable. Il est donc important que le responsable sécurité travaille en étroite collaboration avec le responsable des risques et/ou de la qualité.

Les établissements voient au travers de cette organisation unique des avantages en matière de pilotage et de coût.

6 - LE PILOTE DE LA DEMARCHE DE SECURITE DU SI

La personne en charge du pilotage de la démarche sécurité assure les rôles suivants :

- Suivre les risques sur le système d'information et informer la Direction Générale.
- Piloter et suivre l'exécution du plan d'action de sécurité du SI.
- Produire un tableau de bord sécurité : définir, collecter, suivre des indicateurs de sécurité et les relier aux risques sur l'activité de l'établissement.
- Assurer une veille réglementaire relative à la sécurité des systèmes d'information.
- Animer l'instance de pilotage de la sécurité du SI.
- Veiller à la prise en compte de la sécurité en amont des nouveaux projets SI.
- Organiser des audits et contrôles sur différents composants et processus du SI pour vérifier le niveau de sécurité et la conformité réglementaire.

Les établissements rencontrés dans le Nord Pas de Calais indiquent que le **qualiticien** peut être un bon candidat, dans une première étape, s'il est difficile de trouver un profil adapté.

- Il est en général rattaché à la Direction ce qui lui donne sa légitimité.
- Sa compétence est transverse et lui donne une bonne connaissance des personnes et de l'organisation de l'établissement.
- Il a acquis une culture du risque et applique des méthodes de gestion des risques dans d'autres domaines que la sécurité du SI.

Toutefois l'expertise technique reste nécessaire pour avoir un avis clair sur les priorités des actions à mener (par exemple, faire le tri entre ce qui est réellement efficace et rentable et ce qui relève du marketing commercial), pour connaître les tendances, pour faire des bons choix entre les différents solutions et architectures de sécurité, pour être légitime dans les actions de sensibilisation, et pour être capable de faire un audit interne pertinent de la sécurité.

Des connaissances juridiques et la capacité à établir des contrats avec les fournisseurs sont aussi nécessaires.

Les compétences techniques ne pèsent pas nécessairement dans le choix. Il pourra s'appuyer sur des expertises techniques présentes dans le service informatique, apportées par le correspondant sécurité (voir ci-dessous).

7 - L'ORGANISATION A METTRE EN PLACE AUTOUR DU PILOTE DE LA DEMARCHE

Pour assister le pilote de la démarche, un correspondant au service informatique est nécessaire

Le **correspondant sécurité** est en général au service informatique ; il assure les fonctions suivantes :

- Coordonner les actions de sensibilisation à la sécurité.
- Aider la réalisation d'un tableau de bord sécurité.
- Maintenir à jour la documentation technique de sécurité.
- Réaliser les actions techniques de sécurité incombant à la DSI, et assurer le support opérationnel en cas d'incident.
- Rendre compte au pilote de la démarche des incidents de sécurité et de l'avancement des actions.
- Organiser la veille sur la sécurité technique.

- Assurer le contrôle et le suivi des interventions des prestataires externes sur le système informatique.

Remarque 1 : les fonctions de correspondant sécurité et de pilote de la démarche peuvent être regroupées ; mais cela nécessite à la fois des compétences techniques informatiques (maîtrise d'œuvre sécurité), et la capacité à pouvoir spécifier les besoins en sécurité et conduire des projets transverses dans l'établissement (maîtrise d'ouvrage sécurité).

Remarque 2 : la fonction de correspondant sécurité exige une expertise technique ; le partage de cette compétence entre plusieurs établissements est conseillé.

Le **comité de pilotage** est animé par le pilote et présidé par la Direction. Il regroupe la DRH, la Direction juridique, les services généraux et techniques et également un représentant pour chaque service dont les activités dépendent fortement du système d'information. Cette instance dispose des rôles suivants :

- Revue et arbitrage sur les actions de sécurité ne relevant pas uniquement de la technique informatique.
- Revue des incidents et des alertes de sécurité de l'information.

Fiche n°6 : La sécurité avant d'autres projets : le bon arbitrage

L'un des freins le plus souvent évoqué dans les retours d'expérience recueillis auprès des établissements, est le fait que la sécurité doit être mise en œuvre au détriment d'autres projets. Un arbitrage est donc nécessaire.

« L'absence de ressources ou de moyens financiers ne peut justifier une négligence notoire du niveau de sécurité au regard des enjeux ».

1 - L'ARBITRAGE DES PRIORITES DES ACTIONS DE SECURITE

Il y a un arbitrage à faire entre les actions de sécurité identifiées et le budget. Les éléments apportés par l'analyse de risques (Cf. *Fiche 5*), le rapport cout/efficacité des actions envisagées peuvent aider à faire cet arbitrage **en toute connaissance de cause**.

Ainsi, en début de démarche, le diagnostic (Cf. *Fiche 5*) consiste :

- à identifier la liste des écarts entre la sécurité du SI estimée par l'état des lieux dans l'établissement et la réalité des bonnes pratiques.
- à identifier les incidents que les utilisateurs rencontrent sur le terrain.

Pour chaque écart ou incident remonté, un plan d'actions palliatives et/ou correctives peut être établi. L'arbitrage entre les actions consiste à conduire deux réflexions complémentaires :

- identifier les **actions immédiates et à bas coûts** (ou « quick-win »).
- identifier les **risques de ne pas agir.**

Parce que les couts ne peuvent être évalués selon une méthode rigoureuse d'analyse, certains établissements rencontrés pour engager la démarche, ont consacré un part du budget SI à la sécurité.

Ils engagent ainsi quelques dizaines de milliers d'euros la première année pour réaliser les premières étapes, sans réserver de ressources importantes.

Ils reconduisent ce budget chaque année dans une optique d'amélioration progressive et continue du niveau global de sécurité.

2 - ARBITRAGE GUIDE PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

Il n'est pas toujours nécessaire de disposer d'un budget important pour améliorer significativement le niveau de sécurité de l'établissement.

Il faut d'abord privilégier les actions qui répondent à, au moins deux, des qualités suivantes : les moins coûteuses, les plus courtes, les moins contraignantes pour les utilisateurs du SI, les plus bénéfiques « rentables ». Elles sont dites des actions « pépites ».

Ces actions « pépites » permettent à la fois d'augmenter significativement le niveau de sécurité, et de communiquer comme autant de « succès » bénéfiques de la démarche.

2.1 - Des actions de bon sens mais à accompagner

Les actions « pépites » sont souvent considérées comme des actions de bon sens ; mais elles peuvent apporter de nouvelles contraintes à l'utilisateur que celui-ci peut refuser. Leur mise en œuvre peut donc être délicate ou impossible si elles sont insuffisamment justifiées par la Direction et accompagnées par les équipes en charge de leur déploiement (voir ci-dessous quelques exemples). Le choix de ces actions doit être confronté aux pratiques du terrain dans un esprit de compromis entre la contrainte et le bénéfice apporté.

2.2 - Quelques exemples de « pépites »

Supprimer les étiquetages des locaux critiques pour éviter d'attirer l'attention de personnes mal intentionnées.
Fermer à clé les salles hébergeant les serveurs informatiques.
Activer les écrans de veille et le verrouillage du poste à la sortie de la veille.
Demander aux utilisateurs ou au support de premier niveau de faire remonter en un point unique les incidents opérationnels et de sécurité. Etablir des rapports périodiques sur les incidents.
Déplacer les cartouches de sauvegarde pour qu'elles ne soient plus au même endroit que le robot de sauvegarde.
Définir des fiches de postes pour tout le personnel du service informatique, intégrant les rôles et obligations en matière de sécurité.
Interdire un usage non professionnel et abusif des ressources informatiques (exemple, téléchargement de musiques ou de films etc.).
Communiquer périodiquement sur les règles de sécurité à respecter au quotidien et sur le guide d'usage des moyens informatiques.
Remplacer les identifiants génériques des administrateurs par des identifiants nominatifs.
Revoir les droits d'accès aux répertoires partagés contenant de l'information à caractère personnel.
Formaliser les procédures d'intervention à distance sur l'informatique de l'établissement

3 - ARBITRAGE PAR LES RISQUES

La deuxième réflexion consiste à se fixer des priorités parmi les incidents auxquels l'établissement est susceptible de devoir faire face, et les prises de risques acceptées « en toute connaissance de cause ».

Bénéfices de l'analyse de risques constatés dans la région Nord Pas- de Calais : *« Les directeurs et médecins ont du mal à percevoir les conséquences potentielles des risques SSI. Ils n'en sont pas conscients ou considèrent qu'il s'agit d'une tâche dédiée au service informatique et n'investissent pas la démarche. »*

L'arbitrage par les risques permet de prendre les meilleures décisions possibles en comparant le risque de ne pas faire et le budget nécessaire pour réaliser l'action de sécurité.

Les résultats du diagnostic ont d'abord permis d'identifier les écarts entre le niveau de sécurité constaté dans l'établissement et l'état de l'art en matière de sécurité. L'analyse de ces écarts permet de déterminer le risque que prend l'établissement à ne pas agir. Attention, **cette analyse demande une réflexion de sécurité partagée avec les utilisateurs du SI pour déterminer la gravité et la vraisemblance des potentiels scénarios d'exploitation de ces faiblesses**.

- Pour éviter toute paranoïa ou naïveté, il faut une bonne expérience des sources de menaces pesant habituellement sur des systèmes d'information analogues pour juger de la vraisemblance des scénarios (sinistres, pannes matériels, bogues logiciels, actions de hackers, de personnels mal intentionnés, etc.).

- Pour juger des conséquences opérationnelles, il faut disposer d'une vision précise et globale du système d'information et comprendre sa place dans le quotidien des utilisateurs. Par exemple, si une information a été involontairement modifiée, quelles sont les conséquences sur la prise en charge du patient ? Si le logiciel de gestion de la restauration est défaillant, quelles sont les conséquences potentielles et dispose –t- on d'une solution de secours ou dégradée ?

L'arbitrage revient à répondre à la question : « Les conséquences du risque, s'il se produit, sont-elles acceptables –par l'institution et par les professionnels de santé- si on choisit de ne mener aucune action pour les prévenir ou pour en réduire les impacts ?».

Formulation des analyses de risques - *CHG de Cornil :* *« Les éléments qui conduisent aux arbitrages doivent être partagés au sein de l'établissement. Il est donc indispensable que les conclusions de l'analyse soient formulées en utilisant un vocabulaire adapté à des non initiés »*

4 - UNE BONNE PRATIQUE BUDGETAIRE

Une bonne pratique est de considérer la sécurité du SI non pas comme un projet autonome, avec un début et une fin, mais comme des actions récurrentes auxquelles est associé un budget annuel. D'autant que les menaces évoluent chaque année et que les décisions doivent être périodiquement réévaluées.

Cette approche d'amélioration continue permet une optimisation des budgets alloués à la sécurité du SI (et d'éviter un pic la première année).

La sécurité doit être intégrée systématiquement en amont à chaque évolution du système d'information. Cette démarche permet une réduction des dépenses car il est beaucoup plus onéreux de réaliser un projet de sécurisation sur un dispositif existant que de sécuriser chaque élément au moment de son acquisition (en intégrant des exigences sécurité techniques et contractuelles dans les cahiers charges) puis postérieurement au cours de son intégration et de son déploiement.

Fiche n°7 : Les facteurs clés de succès de la démarche

1 - Le point de depart de la maitrise de la Securite du Systeme d'Information

1) **Viser des objectifs de sécurité qui répondent aux besoins de l'établissement**, (Cf. *Fiches 2 et 4*).

2) **Fixer des trajectoires atteignables** (Cf. *Fiches 4 et 5*).

3) **Prévoir l'organisation et le pilotage de la démarche de sécurité** (Cf. *Fiche 5*)

2 - La vision globale portee par la Direction

La sécurité du SI doit être vue globalement et ne pas être **considérée comme une suite non coordonnée de projets techniques autonomes.**

Il faut :

- garder en vue que des solutions organisationnelles et/ou contractuelles, sont parfois plus adaptées que des moyens purement techniques parfois chers ou contraignants.
- éviter des contraintes trop fortes ou des incompatibilités avec les usages des utilisateurs du SI ; la sécurité ne va pas à l'encontre des usages. Elle donne les moyens d'aller vers des nouveaux usages, en mettant en place la confiance qui convient.
- mener une sensibilisation régulière et générer ainsi des réactions réflexes en matière de sécurité.

Comme le souligne le Syndicat Interhospitalier du Limousin : *« Il ne faut pas se focaliser uniquement sur l'aspect technique et ne faut pas sous-estimer l'aspect organisationnel d'un projet de sécurité SI qui est souvent important et impactant »*

La sécurité n'est pas qu'un projet informatique. Elle doit être portée par la Direction car elle implique la participation de l'ensemble des utilisateurs du système d'information.

3 - L'adhesion des utilisateurs doit etre un point d'attention majeur

L'importance de l'organisation et la communication - *CHG de Cornil* : *« L'organisation et la communication sont les 2 facteurs essentiels pour la mise en œuvre d'une démarche de sécurité SI ».*

Ce sont souvent les erreurs humaines des utilisateurs dans l'établissement qui sont à l'origine des incidents, du fait de négligence ou d'ignorance. Une communication ciblée et régulière **sur les risques et les enjeux**, permet de conserver la vigilance des acteurs, et à chacun de se sentir concerné (Cf. *Fiche 8*).

4 - La demarche securite est imperative meme si aucun incident ne s'est produit

Si la survenance d'incidents de sécurité est un indicateur pertinent dans le pilotage de la sécurité, il doit toujours être considéré avec prudence.

Des dossiers patients nouvellement exposés – *Groupe de cliniques* : *« Un piège consiste à croire que la sécurité est assurée car rien ne s'est produit. Il est important de noter que l'arrivée du DPI apporte une valeur supplémentaire aux données présentes en établissement, et qu'elles deviennent, de fait, une cible intéressante. »*

Exemple avéré : « un établissement a subit un chantage suite à une attaque en exploitant un accès externe via une machine de radiothérapie et entrainant le vol de dossiers patients. »

En effet, tous les incidents survenus ne sont pas forcément détectés, car souvent les attaques ne laissent pas nécessairement de trace (consultation ou vol de données par exemple) ou bien les utilisateurs du SI les gèrent localement et ne les déclarent pas.

Ainsi, les deux axes de réflexion à la base de la démarche sécurité du SI sont :

- Quels sont les incidents susceptibles de se produire et quelle démarche proactive peut-on mettre en œuvre pour les éviter?
- Comment réagir et contenir l'incident s'il se produit ?

La **connaissance des risques** qui peuvent peser sur le système d'information de l'établissement est un passage obligé de la démarche. Alors, le bien connu « mieux vaut prévenir que guérir » se vérifie généralement.

La prévention est indispensable – *Groupe Vitalia :* *« les actions de prévention sont à mettre en place pour éviter ou limiter les impacts d'un incident. Par exemple, la procédure permettant de mobiliser un administrateur le week-end en cas d'incident grave est un élément de coût faible et qui peut considérablement limiter les impacts d'un incident de production »*

5 - IL EST NECESSAIRE DE DOCUMENTER LA DEMARCHE

La sécurité passe avant tout par le respect de règles et de bonnes pratiques ; les règles de sécurité doivent être considérées comme naturelles et réalisables avant de documenter ces pratiques; et il vaut toujours mieux appliquer de bonnes pratiques de sécurité non documentées que d'avoir une documentation élaborée mais non suivie.

La documentation est nécessaire - *CHG de Cornil :* *« Il faut trouver un équilibre entre l'écrit et l'oral »*

Certains documents tels que la Politique de Sécurité du SI, et les plans d'action sécurité sont incontournables pour formaliser l'organisation et les responsabilités dans la démarche. (Cf. *Fiche 9*). La documentation des procédures de sécurité existantes contribue à la qualité de l'application des règles et permet d'éviter les dérives des pratiques. Toutefois, il est important, de ne pas considérer que la sécurité est assurée par la publication d'un document, et que les recommandations qui y sont faites, seront suivies. C'est pourquoi la production de documents de sécurité doit être accompagnée de :

- Communications ciblées pour faciliter leur appropriation.
- Vérifications qu'ils sont compris des personnes en charge de les appliquer.
- Contrôles et audits pour que les recommandations soient effectivement respectées.

UNE IDEE FAUSSE : LA SECURITE DU SI EST UN SUJET TECHNIQUE ET COMPLIQUEE QUI NE PEUT ETRE TRAITEE QUE PAR L'INFORMATIQUE

Une idée fausse mais néanmoins répandue est que la sécurité est compliquée et doit être réservée aux seuls experts de l'informatique qui s'en occupent en autarcie.

Au début de la démarche, des actions simples et non techniques dont l'application peut ne pas relever de la DSI permettent d'augmenter significativement le niveau de sécurité d'un établissement (Cf. *Fiche 6*).

Des mesures parfois simples et peu couteuses - *CH. Cornil* : *« Fermer à clé le local contenant les serveurs est avant tout une action de bon sens permettant de limiter un grand nombre de risques»*

Ensuite, des projets sont mis en œuvre qui ont un impact sur l'organisation: gestion des identités et des accès des utilisateurs au système d'information, plan de continuité et plan de reprise

6 – ECHANGE ET MUTUALISATION AVEC D'AUTRES ETABLISSEMENTS

Il est intéressant, dans le cadre d'une démarche sécurité, d'échanger avec d'autres établissements. Le Directeur peut ainsi :

- Inciter le Responsable de la Sécurité du Système d'Information à travailler en équipe avec d'autres collègues d'établissements de la région, par exemple, pour établir des chartes ou autres livrables communs.
- Faciliter la structuration de l'activité de Sécurité SI sur la région, le territoire.
- Contacter d'autres établissements pour partager et utiliser l'expérience des solutions mises en œuvre, et pour pouvoir se « benchmarker ».

Une communication enrichissante entre établissements - *CHG de Cornil :* *« Chaque établissement est autonome. Cependant, il existe un effet d'entraînement entre les établissements, en particulier en termes de démarche SSI. Chaque établissement rencontre des problématiques similaires et se pose les mêmes questions. »*

La réalisation d'actions similaires par plusieurs établissements permet d'envisager une éventuelle mutualisation des compétences. La mutualisation entre établissements de santé ne dédouane cependant pas d'un pilotage local de la démarche.

D'autres aides extérieures peuvent être utilisées (Cf. *Fiche 2*).

Fiche n°8 : La communication : un levier essentiel

Communiquer auprès des utilisateurs est une priorité, car les usages qu'ils font du système d'information sont à l'origine de la majorité des incidents de sécurité :

- **Oublier un document sur une imprimante ;**
- **Stocker des fichiers sans se préoccuper des sauvegardes ;**
- **Installer des applications informatiques sans prévenir le responsable des Systèmes d'Information ;**
- **Identifier des erreurs sans faire remonter l'information ;**
- **Considérer que se préparer à faire face à un arrêt temporaire de l'informatique est une perte de temps ;**
- **Utiliser une messagerie non sécurisée pour transmettre (hors de l'établissement) des informations médicales sur un patient.**

Tous ces exemples sont autant de comportements risqués qui peuvent être évités par une action adaptée et régulière d'information.

Selon la grande majorité des RSSI, la plus grande menace à laquelle doit faire face le SI est le comportement négligent ou malveillant de l'être humain.

1 - LA COMMUNICATION DOIT VISER UN DOUBLE OBJECTIF

La communication vise à sensibiliser **régulièrement** les utilisateurs sur leurs responsabilités dans le cadre de l'usage du SI et à les former à l'utilisation des moyens de sécurité disponibles :

- **Informer le personnel** de l'établissement de la politique de sécurité.
- **Maintenir la vigilance** du personnel quant à son usage de l'informatique.

1.1 - Informer les personnels de l'établissement

Dès le lancement de la démarche sécurité, il est nécessaire de **communiquer sur les enjeux de la démarche elle-même**. Il faut, en effet, veiller à ce qu'une action de sécurité ne soit pas perçue comme une nouvelle contrainte dans le quotidien ou comme un moyen intrusif pour effectuer des contrôles sur l'activité du personnel.

Le retour d'expérience des établissements montre qu'une communication périodique en rappelant les enjeux, la finalité et la place de tous est indispensable pour la pérennité de la démarche.

1.2 - Maintenir la vigilance

Des messages simples et courts, destinés à tous les membres de l'établissement, permettent de rappeler les **bonnes pratiques de sécurité** et d'**alerter sur les incidents vécus ou juste évités**. La récurrence de ces actions est indispensable pour maintenir la vigilance et de faire de la sécurité un réflexe au quotidien.

Inversement, il faut permettre aux utilisateurs de s'exprimer sur les difficultés vécues sur le terrain pour appliquer les règles imposées. Ceci permet de trouver un meilleur compromis entre sécurité et contraintes opérationnelles.

La communication de retours d'expérience sur les incidents vécus par d'autres établissements est également un très bon vecteur de sensibilisation et de maintien de la vigilance.

2 - LES AXES DE COMMUNICATION

Les actions de sécurité (celles qui ne sont pas strictement techniques) doivent être présentées en mettant en avant le rôle joué par chacun dans leur mise en œuvre et en rappelant que des reflexes simples peuvent aider à la sécurité du système d'information :

- « Partagez les informations en toute sécurité dans des répertoires de fichiers partagés (ne stocker qu'exceptionnellement des informations sur des clés USB) ».
- « Respectez les règles d'usage des cartes CPS et des mots de passe ».
- « Soyez vigilant quand votre un interlocuteur ou un email vous demande votre mot de passe applicatif ».
- « Protégez votre édition papier ».
- « Signalez toute suspicion d'incident, tout oubli peut aggraver la situation ».
- « Ne connectez pas une clé USB sans être sûr de son origine ».
- « Ne stockez pas vos fichiers sur des sites en ligne ».
- « Ne cliquez pas sur les des liens contenus dans des emails ».

Les exemples de messages de communication doivent être adaptés à la fonction des interlocuteurs.

Les messages doivent être ciblés selon les interlocuteurs. A titre illustratif, voici la liste ci-dessous des **principaux messages** de communication utilisés par les établissements du Limousin, pour **accompagner un projet de gestion des accès**.

- **A destination des médecins et infirmiers** : la carte professionnelle de santé appartient à son porteur. Il s'agit d'une carte d'identité professionnelle et non pas simplement d'un outil technique servant à se connecter à l'informatique de l'établissement.

- **A destination de l'ensemble du personnel interne** : les outils mis en place et les traces générées ne sont pas utilisés pour vérifier les heures de connexions ou le temps passé dans l'établissement. Il s'agit au contraire d'un dispositif dont la finalité est de protéger le travail des agents en évitant notamment qu'on puisse agir dans le système d'information en leur nom. Il permet également d'analyser l'origine d'anomalies éventuelles afin d'éviter qu'elles se reproduisent.

- **A destination des membres de la DRH :** Les ressources humaines sont au cœur de la confiance dans le système de gestion des accès. Elles sont responsables de l'identité des personnels, elles sont informées de leur fonction dans l'établissement. A ce titre, elles sont responsables du maintien à jour de l'annuaire des personnes qui est le socle de base du contrôle d'accès des utilisateurs et des habilitations.

3 - Le Directeur de l'établissement doit soutenir cette communication

L'engagement du Directeur dans cette communication comme dans la démarche sécurité, est indispensable à leur légitimité et à l'adhésion de tous aux bonnes pratiques.

4 - Les principes generaux de communication

La communication autour de la Sécurité SI n'est pas différente de toute autre démarche de communication.

Ressentis collaborateur	Facteurs de résistance	Axes de communication
« Je n'ai pas le temps d'en prendre connaissances »	Document dense et long	Rythme de communication séquencé
« Je n'ai pas envie de lire »	Document formel et magistral	Format attractif (animation, illustration,…)
« Ca ne me concerne pas directement»	Document générique	Message adapté aux cibles
« Je ne vois pas les bénéfices immédiat dans mon activité quotidienne »	Document d'intérêt général	Message adapté aux cibles
« Je suis tout seul avec mon document, je n'ai personne pour en parler, pour m'expliquer »	Manque de communication orale autour de la PSSI	Message oral relayé par l'encadrement
« Je n'aime pas me conformer aux normes »	Document règlementaire décliné en règles et procédures	Format attractif

5 - La communication vers les intervenants dans le SI, externes a l'etablissement

Quand un intervenant externe doit avoir accès au système d'information, il est nécessaire de lui communiquer les règles à respecter relativement à la sécurité SI afin d'assurer le respect de la politique et des normes de l'établissement en la matière. Outre le fait que son intervention au sein de l'établissement doit être contrôlée, il doit appliquer les règles de sécurité, au même titre qu'une personne interne à l'établissement.

Cette communication intervient en complément des règles de sécurité qu'il faut prévoir de façon formelle dans les contrats de prestations.

Fiche n°9 : La documentation sécurité : un minimum est nécessaire

Documenter la sécurité est un effort indispensable pour pérenniser la démarche.

L'existence d'une documentation n'est pas le gage d'une sécurité adaptée ; quelques établissements disposent d'un document de politique de sécurité qui ne reflète en rien leur niveau de sécurité du système d'information. Aussi, un juste équilibre doit être trouvé entre le niveau de formalisation et les actions opérationnelles.

1 - LE SOCLE MINIMAL DE FORMALISATION DE LA SECURITE

1. La **cartographie des risques** pesant sur les applications du SI (ou appelé cartographie des besoins de sécurité).
2. La **Politique de Sécurité** du Système d'Information de l'établissement (notée PSSI par la suite).
3. La **charte d'utilisation** des moyens informatiques et de télécommunication.
4. Les **procédures opérationnelles** et **techniques** de sécurité.
5. **Plan d'action** pluriannuel dédié à la sécurité du Système d'Information (ou plan de sécurité informatique).

Au-delà des documents propres à la sécurité du SI, la bonne tenue par la DSI des **documentations relatives au SI** (schéma d'architecture et du réseau, plan d'adressage et de nommage, inventaires des applications et des interfaces, etc.) est un élément important contribuant à la sécurité.

1.1 - La cartographie des risques

La cartographie des risques est la constitution et le maintien d'un **référentiel décrivant, pour chaque domaine fonctionnel du SI, les enjeux et besoins de sécurité associés**. Il fournit une vision globale des éléments critiques du SI. Elle peut constituer un tableau de bord de suivi et de justifications des arbitrages sur la sécurité.

En pratique, les utilisateurs du SI (médecins et soignants) doivent formaliser une réflexion :

- Quel est le niveau maximal acceptable de **perte définitive de données** dans l'application informatique compte tenu de son utilisation?
- Quelles sont les conséquences financières, juridiques, ou opérationnelles en cas de **mise hors d'état temporaire de fonctionnement** de l'application ?
- Quelles sont les conséquences sur la qualité des soins en cas de **modification anormale des données** ou en cas de mise hors d'état temporaire de fonctionnement de l'application ?
- En cas de **divulgation d'informations**, quel est son impact sur le service et/ou sur les personnes concernées ?
- Est il nécessaire de tracer et de conserver l'historique des actions ayant conduit à une modification illégitime de données ?

1.2 - La Politique de Sécurité du Système d'Information de l'établissement (PSSI)

La Politique de Sécurité du SI constitue le **cadre de local de référence et de cohérence** en matière de sécurité de l'information dans un établissement.

La PSSI de l'établissement s'appuie notamment sur les principes fondateurs de :

- La PGSSI-S, Politique Générale de Sécurité des Systèmes d'Information de Santé – En cours de rédaction et qui sera disponible sur le site de l'ASIP Santé fin 2013.
- La PMSSI, politique ministérielle de sécurité du SI (Ministère de la Santé).

La PSSI détaille la réflexion de l'établissement relative à la sécurité SI ; on y retrouve :

- Le périmètre du SI dans l'établissement.
- Les besoins de sécurité (basés sur le rappel des normes et textes réglementaires à respecter, les menaces auxquelles l'établissement est confronté, les failles identifiées, etc.).
- Les priorités et les buts à atteindre.
- L'organisation sécurité du SI ainsi que les rôles et responsabilités des intervenants.
- La description des processus ci-dessous :
  - L'analyse des risques de sécurité du SI.
  - La gestion des identités et des accès des utilisateurs du SI.
  - Le plan de continuité et de reprise d'activité.
  - La gestion d'incidents de sécurité.
  - Le contrôle de la sécurité.
  - La communication / sensibilisation.

La PSSI n'est pas nécessairement un document unique mais peut être le regroupement d'un document cadre et de politiques plus techniques.

Enfin, c'est un document qui doit évoluer dans le temps pour accompagner l'évolution de maturité de l'établissement en matière de sécurité.

1.3 - La charte d'utilisation du système d'information et de télécommunication

La charte d'utilisation du système d'information et de télécommunication est un document essentiel dans la mise en œuvre d'une démarche sécurité : **elle contribue à la responsabilisation de chacun et est le seul document de portée juridique, dès lors qu'elle est annexée au règlement intérieur de l'établissement**.

Celle-ci présente les droits et devoirs liés à l'utilisation, par tous les acteurs (salariés ou non), des ressources informatiques et de télécommunication au sein de l'établissement.

Elle doit permettre d'assurer à chacun l'utilisation optimale des ressources informatiques et de télécommunication compte tenu des exigences de sécurité.

Elle vise également à concilier, d'une part, le respect de la vie privée des utilisateurs du SI, leurs droits et libertés individuelles (comme par exemple, le secret de leurs correspondances privées), et d'autre part, le nécessaire droit de contrôle par la direction de l'usage des outils professionnels mis à la disposition des utilisateurs dans l'optique d'éviter abus et dérives.

Les règles décrites ont pour vocation d'assurer à chacun l'utilisation des ressources informatiques dans le strict respect de la loi et de l'éthique.

Elle peut être complétée par des documents visant des usages particuliers (télétravail) ou des populations spécifiques dont les droits et devoirs en matière de sécurité diffèrent du reste du personnel par les privilèges qu'ils ont sur le SI (administrateurs, prestataires, intervenants en télémaintenance sur le SI …).

1.4 - Les procédures opérationnelles et techniques de sécurité

Les procédures opérationnelles et techniques de sécurité décrivent les actions concrètes visant à protéger le SI de l'établissement et à maintenir le niveau de sécurité.

La rédaction de ces procédures est souvent faite lors d'une action d'amélioration des procédures existantes. Elles sont destinées aux équipes SI et aux experts métiers.

1.5 - Le plan d'action pluriannuel dédié à la sécurité des SI

Le plan d'action de la sécurité des SI peut être intégré à un plan d'action général des SI. Les actions cibles portant sur la sécurité doivent apparaitre en relation avec les besoins de sécurité mis en avant par les médecins et soignants. Les actions doivent être priorisées.

C'est dans le plan d'action de sécurité que l'on peut trouver notamment les informations sur la planification des tests de secours, de continuité et de reprise du SI.

Fiche n° 10 : Les coûts de la sécurité

Le budget d'une démarche sécurité dépend fortement du contexte local. Toutefois, pour fournir des ordres de grandeur, cette fiche présente des budgets constatés dans des établissements, et des tarifs de prestations extérieures recueillies par un groupement d'achat.

Attention : les chiffres indiqués dans ce document sont issus de retours d'expérience d'établissements durant la période 2009-2013. Ces données ne peuvent être utilisées ou reproduites sans l'autorisation écrite de la DGOS.

1 - Un budget global difficile a chiffrer precisement

L'essentiel du coût pour la mise en œuvre de la démarche sécurité du SI porte sur des moyens humains : expertise externe et personnels de l'établissement. Il y a peu d'achats de fournitures (matériels ou logiciels).

Bien entendu, cette règle ne s'applique pas aux chantiers les plus complexes, tel que l'installation d'une salle informatique ou le contrôle des accès des utilisateurs en utilisant la carte CPS (Cf. *Fiche 3* le paragraphe « la sécurité une démarche itérative faite de plusieurs projets »).

Il est difficile d'estimer les coûts de la sécurité SI. Les retours d'expérience d'établissements montrent des variations importantes. Ces variations sont liées à la situation initiale, au périmètre considéré, aux orientations retenues par l'établissement (externalisation, réalisation en interne, etc.).

2 - Une bonne pratique budgetaire

Une bonne pratique est d'allouer un **budget annuel global à la sécurité du SI**. Celle-ci repose sur une démarche dite d'amélioration continue incluant des actions récurrentes ; il ne s'agit donc pas d'un projet avec un début et une fin. Cette pratique a l'avantage de lisser sur plusieurs années le budget alloué à la sécurité du SI et d'éviter ainsi un pic la première année.

3 - Un budget securite dans les projets d'evolution du SI

Une autre bonne pratique est de répartir les coûts de sécurisation dans chaque projet de développement du SI ; elle consiste à prévoir dans chaque projet SI, une part du budget aux aspects de sécurité. L'avantage d'intégrer cette réflexion sécurité au sein des projets SI est qu'elle réduit les dépenses ; en effet, il est toujours plus onéreux de sécuriser un existant que de sécuriser chaque élément avant leur déploiement.

> Cette part est en moyenne de l'ordre de 6% à 12% du budget du projet SI selon son importance et son exposition aux menaces (connexion à l'Internet, utilisation de nouvelles technologies, etc.).

4 - Le diagnostic de la situation, la mise en place d'une gouvernance de la SSI et d'une PSSI

Les démarches menées dans la région du Nord Pas de Calais ont consisté pour chaque établissement à réaliser un diagnostic de la sécurité SI, un plan d'action détaillé, puis le lancement des actions de sécurité. Le coût de l'assistance externe se situe en moyenne entre 12 000€ et 17 000€ selon la taille de l'établissement (entre 75 et 150 lits). Les délais de réalisation ont été de 2 à 3 mois.

> Le prix forfaitaire moyen complet est estimé entre 28.000 € et 34.000 € selon la taille de l'établissement (entre 100 et 500 lits). Il inclut l'accompagnement à la mise en œuvre du plan d'action notamment la rédaction d'un corpus documentaire.

Ces coûts correspondent aux prestations externes et n'incluent pas la mobilisation des personnes internes à l'établissement nécessaire à l'accomplissement de la démarche (ateliers de travail, réunions de revue et d'arbitrage).

5 - La realisation des premieres actions du plan d'action

Les retours d'expérience des démarches sécurité réalisées dans les établissements du Nord Pas de Calais (entre 75 et 150 lits) montrent que les premiers travaux durant les 2 premiers mois nécessitent une charge de l'ordre d'1,5 ETP: 1 ETP pour le responsable de la démarche et 0,5 ETP répartis entre les autres parties prenantes.

6 - Une charge de travail repartie pour la realisation des actions securite

En fonctionnement nominal, la charge interne liée à la réalisation des actions transverses de sécurité et au traitement des incidents de sécurité dans **un établissement** (entre 100 et 500 lits)**est évaluée entre 0,3 et 0,5 ETP**.

Des journées d'expertise peuvent être achetées auprès de prestataires spécialisés. Selon Uni-HA, les **prix du marché s'établissent en moyenne à 850 € par jour** (frais de déplacement inclus).

Les projets plus complexes ne sont évidemment pas compris dans ces charges.

7 - LES COUTS D'UN PROJET DE SECURISATION DES INFRASTRUCTURES

La sécurisation de l'infrastructure des serveurs informatiques et du réseau est l'une des priorités pour garantir la continuité du SI. Les investissements sont en général assez lourds.

Le groupe Vitalia estime entre 70 000 et 250 000 € l'investissement pour la construction d'une salle pour les serveurs informatiques et la mise à niveau de l'infrastructure du réseau.

8 - LES COUTS D'UN PROJET DE GESTION DE LA CONFIDENTIALITE DES DONNEES MEDICALES

Un projet de gestion de la confidentialité des données médicales consiste à mettre en place une gestion des identités des utilisateurs du SI (incluant l'annuaire des personnels de l'établissement), une gestion des droits d'accès aux applications du SI et des moyens techniques d'authentification (cartes CPS).

Les couts d'un tel projet concernent principalement la mobilisation de ressources humaines (60%). Ce projet demande des prestataires spécialisés pour assister l'établissement dans la mise en place de la solution sur le plan organisationnel et technique.

Pour un établissement entre 300 et 500 lits (chiffres issus des offres reçues dans le cadre des marchés Uni-HA/NTIC/SSI, coordonnés par le CHRU de Lille), les coûts moyens du projet « clés en mains » sont les suivants:

- Prestation d'installation de la solution technique : entre 47 et 140.000 €.
- Licences des logiciels (coût ramené au lit) : entre 80 et 130 €.
- Maintenance annuelle (coût ramené au lit) : entre 20 et 50 €.

Auquel s'ajoute le coût d'une assistance à maîtrise d'ouvrage.

Remerciements

CONTRIBUTEURS

Le guide a été élaboré en s'appuyant sur le retour d'expérience des deux projets régionaux, dans le Nord Pas de Calais et dans le Limousin, qui visent chacun plus d'une vingtaine d'établissements. Ces projets sont pilotés par les syndicats Inter-hospitaliers de ces régions.

Les personnes rencontrées dans la région Nord Pas de Calais sont :

- MM L. Vaurette et P. Flahauw du SIIH5962
- MM T. Aubin du C H de Seclin

Et dans la région Limousin :

- MM Patrick Boisseuil, David Robine et Christophe Baudot du SIL-SIRPC
- MM G. J.-P. Plas et P. Fouche du CH de Cornil
- MM M. Petryszyn et D. Ribeiro du CH de Neris-Les-Bains

Le guide a également bénéficié du retour d'expérience du groupe VITALIA. Les personnes rencontrées sont MM J.M. Culioli et A. Lebez.

La fiche 10 « Les coûts de la sécurité » a bénéficié de données fournies par M Guillaume Deraedt du CHRU de Lille, qui sont extraites de l'estimation du coût de la mise en place d'une gouvernance de la SSI et d'une PSSI, basé sur les offres reçues au titre des marchés Uni-HA/NTIC/SSI.

COMITE DE RELECTURE

Le comité de relecture s'est réuni deux fois. Trois versions du document ont fait l'objet d'une relecture et de commentaires.

Les membres du comité de relecture étaient :

Mmes A. Kempf (CHU de Rouen), S Walz (fondation Hopale), I. Salesse-Lavergne (hôpital St Joseph à Marseille), M. Jarossay (Institut Curie), M.N.Billebot (ANAP), F. Pothier (DGSSI-S).

MM E. Grospeiller (Ministère de la Santé), G. Deraedt (CHRU de Lille), Cedric Cartau (CHU de Nantes), M. Raux (CH de Versailles), P. Boisseuil (SIL), D. Robine (SIL), M. Metz (ASIP santé), P. Duclos (DGOS).