Plan de continuité et de reprise d'activité en environnement hospitalier : CHRU de Brest

Frédéric Cabon

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Mémoire d'ingénieur

Frédéric Cabon

PLAN DE CONTINUITE ET DE REPRISE D'ACTIVITE
En environnement Hospitalier

CHRU DE BREST

Soutenu en septembre 2011

JURY

Président : Monsieur Pollet

Membres : Monsieur Legeas
Monsieur Dupuis

Version 24-06-11

SOMMAIRE

1. PREFACE

1.1 REMERCIEMENTS

Je souhaite tout d'abord remercier tous ceux qui ont contribué directement ou indirectement à l'aboutissement de ce travail.

J'adresse mes remerciements aux collègues de la DSIS pour leur collaboration et pour leur soutien tout au long du projet.

Je tiens à remercier Monsieur Legeas, Directeur de la DSIS pour la confiance qu'il m'accorde et les personnels des services de soins et administratifs sans qui ce projet n'aurait pas de sens, je les remercie pour leur accueil et leur contribution au projet.

Je remercie Eric Dupuis mon tuteur du Centre National des Arts et Métiers pour son soutien tout au long de la réalisation de ce mémoire, pour ses remarques pertinentes et son aide précieuse.

Enfin, mes plus profonds remerciements à ma femme Maryline, pour m'avoir encouragé et soutenu dans les moments difficiles. Son soutien permanent au cours de toutes ces années a été sans nul doute, déterminant pour la finalisation de ce mémoire.

1.2 AVANT PROPOS

Le système d'information hospitalier (SIH) est destiné à faciliter la gestion de l'information médicale et administrative de l'hôpital.

La mission première de l'hôpital, le soin, est de plus en plus interdépendante de la continuité de service du système d'information hospitalier. De ce constat, l'hôpital doit aujourd'hui passer d'une gestion réactive et défensive du risque à une gestion qui se veut pro-active et offensive : c'est dans ce cadre que la notion de plan de continuité d'activité prend tout son sens.

Mon mémoire s'organise de la manière suivante :

Après l'introduction, le second chapitre présente le contexte dans lequel s'est déroulé mon projet d'ingénieur. La définition du projet de mémoire y sera exposée.

Dans le troisième chapitre, je décris tout d'abord les grands principes du plan de continuité et les terminologies associées. Puis, j'expose les cadres normatifs et réglementaires liés au plan de continuité. Enfin, je présente la démarche et les étapes fondamentales nécessaires à la mise en œuvre d'un plan de continuité.

Dans le chapitre quatre, je reviens sur le contexte et la démarche de mon projet, puis par le biais de mon plan d'action, je décris les différentes phases du projet.

Pour conclure, je dresse dans le dernier chapitre, une synthèse du travail réalisé. Enfin, je décris le bilan personnel et les perspectives professionnelles que ce projet m'apporte.

2. CONTEXTE

Mon projet de mémoire se déroule au sein de la DSIS du CHRU de Brest. J'y occupe le poste de technicien supérieur hospitalier depuis quatre ans. Pendant trois ans ma fonction fut d'administrer les éléments composants le SAN, et les serveurs de type UNIX et Linux. Après avoir présenté mon projet de mémoire à ma direction, celle ci m'a proposé d'évoluer vers de nouvelles responsabilités. Depuis le début de l'année 2011, je fais fonction de Responsable Sécurité du Système d'Information et suis directement rattaché à la direction des systèmes d'information de santé. A ce titre, je suis entre autre en charge de la mise en place de la politique de sécurité du CHRU de Brest.

Je présente dans un premier sous chapitre l'hôpital de Brest, l'entreprise où s'est déroulé mon projet d'ingénieur. Dans un second temps, je développe l'organigramme et le fonctionnement du service dans lequel j'ai effectué mon projet. Enfin je décris dans quel contexte j'ai réalisé mon projet de mémoire, le périmètre du projet ainsi que les équipes qui ont contribué au projet.

2.1 PRESENTATION DU CENTRE HOSPITALIER REGIONAL UNIVERSITAIRE DE BREST

Le Centre Hospitalier Universitaire de Brest, premier employeur de la ville avec 6 700 salariés, est un acteur économique de premier plan au service de la Bretagne Occidentale pour une population de 1,3 millions d'habitants. Le CHRU est le premier opérateur de santé de la région avec 6 établissements comptant plus de 2 100 lits, 122 000 personnes hospitalisées chaque année, 432 000 consultants et 65 000 passages aux urgences. Avec 2 833 étudiants inscrits en Faculté de Médecine et des Sciences de la Santé et 600 élèves inscrits dans les écoles paramédicales, le CHRU s'affirme enfin comme un grand pôle de formation et de promotion professionnelle dans la région.

Les Missions du CHRU sont le soin, l'enseignement et la recherche.

Le CHRU répond à la fois à une mission de proximité pour les soins courants et à une mission de recours pour les établissements de santé publics ou privés de la région. Les priorités sanitaires du CHRU sont déterminées par le Schéma Régional d'Organisation Sanitaire. Toutes les spécialités médicales et biologiques (51 au total) sont représentées au CHRU qui assure également le diagnostic et la prise en charge de l'ensemble des maladies rares à travers ses centres de compétences.

Le CHRU de Brest concourt à la formation des futurs médecins et chirurgiens-dentistes qui reçoivent une formation pratique complétant les enseignements théoriques de la Faculté de Médecine et des Sciences de la Santé de Brest

Le CHRU participe également à la recherche biomédicale menée par les équipes reconnues par le Ministère de l'Enseignement Supérieur et de la Recherche, dont deux labellisées INSERM et les laboratoires universitaires de la Faculté de Médecine

2.2 PRESENTATION DE LA DIRECTION DES SYSTEMES D'INFORMATIONS DE SANTES

2.2.1 ORGANIGRAMME DSIS

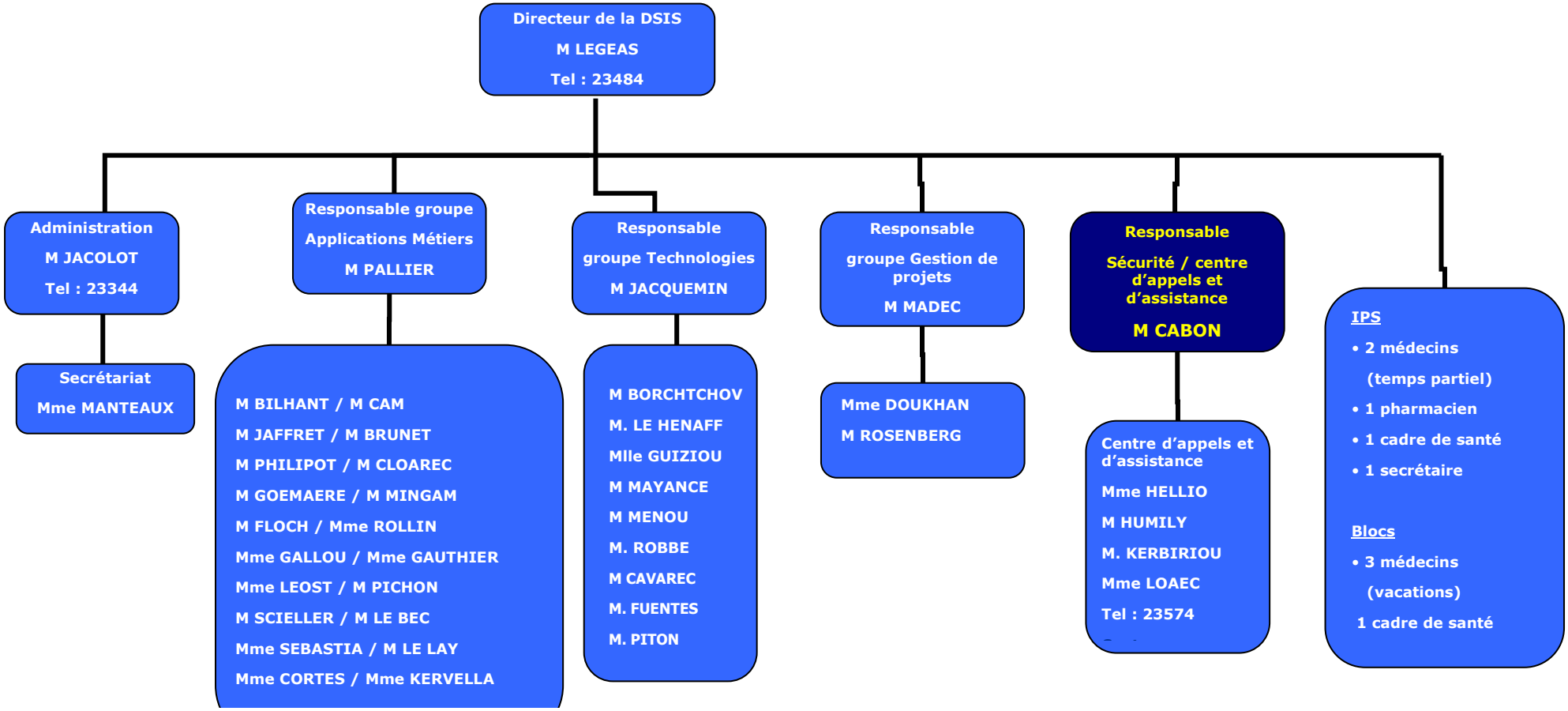


Figure 1 -Organigramme de la DSIS

2.2.2 NOUVELLES MISSIONS

Mes nouvelles missions en tant que RSSI depuis le 1er janvier 2011 sont de :

- Définir les objectifs de la politique de sécurité du SI
- Recenser et analyser les risques inhérents à l'évolution technologique et ses conséquences sur le SI
- Contrôler l'application des règles de sécurité du SI
- Contrôler l'efficacité des plans de secours du système informatique
- Conseiller et assister les équipes informatiques, valider les règles de sécurité au niveau global

Je suis responsable de la centrale d'appels et d'assistance, à ce titre je manage ce groupe. Les points réguliers effectués avec l'équipe help desk, sont pour moi l'occasion de me rendre compte des problèmes récurrents rencontrés sur des éléments de l'infrastructure informatique ou logiciels. Les informations remontées me permettent d'avoir une vision très terre à terre du SI et des problématiques qui y sont liées.

Je suis également responsable des astreintes informatiques du weekend et des soirs de semaines. De ce fait, je suis chargé de faire respecter le protocole d'astreinte et veille à ce que les fiches réflexes informatiques soient à jour.

En tant que correspondant qualité, j'ai été sollicité pour préparer la certification qualité V2010 en animant un groupe de travail sur le critère de la sécurité du système d'information. Je travaille également en étroite collaboration avec la correspondante CNIL et lui apporte mon expertise technique et mes connaissances sur la cartographie du SI. En participant tous les lundis matins à la réunion de direction de la DSIS, cela me permet d'avoir une vision globale des projets en cours et de connaître la stratégie et la politique souhaitée par la direction de l'établissement.

Par mes nouvelles attributions, je fais partie d'un groupe de travail piloté par le GCS (Groupement de Coopération Sanitaire). Ce groupe de travail à pour but la mise en œuvre d'une politique de sécurité régulée au niveau national, sous l'égide de l'ASIP Santé (Agence des Systèmes d'Information Partagés de Santé), et au niveau régional, sous l'égide de l'Agence Régionale de Santé (ARS), visant à déployer les outils de télésanté et à développer l'interopérabilité des systèmes d'information de santé, notamment dans la perspective de la constitution d'un espace numérique régional de santé (ENRS) et du dossier médical personnel (DMP), pour le bénéfice de la prise en charge des patients.

2.3 CONTEXTE DE PLAN DE CONTINUITE ET DEFINITION DU PROJET

La gestion de continuité des activités professionnelles est un des points incontournable de la politique de sécurité du système d'information du CHRU de Brest. Cette politique découle des directives imposées par la PMSSI (Politique Ministériel de Sécurité des Systèmes d'Information)[**1**]. La sécurité des systèmes d'information s'impose comme une composante essentielle de la protection de l'ensemble du périmètre du ministère. Elle relève d'une vision stratégique de chaque organisme ; « La PMSSI peut être définie comme étant l'ensemble formalisé des éléments stratégiques et des principes de sécurité, ayant comme objectif la protection de système d'information » extrait du document de politique générale PMSSI diffusé le 21/01/2011 par le ministère du travail de l'emploi et de la santé.

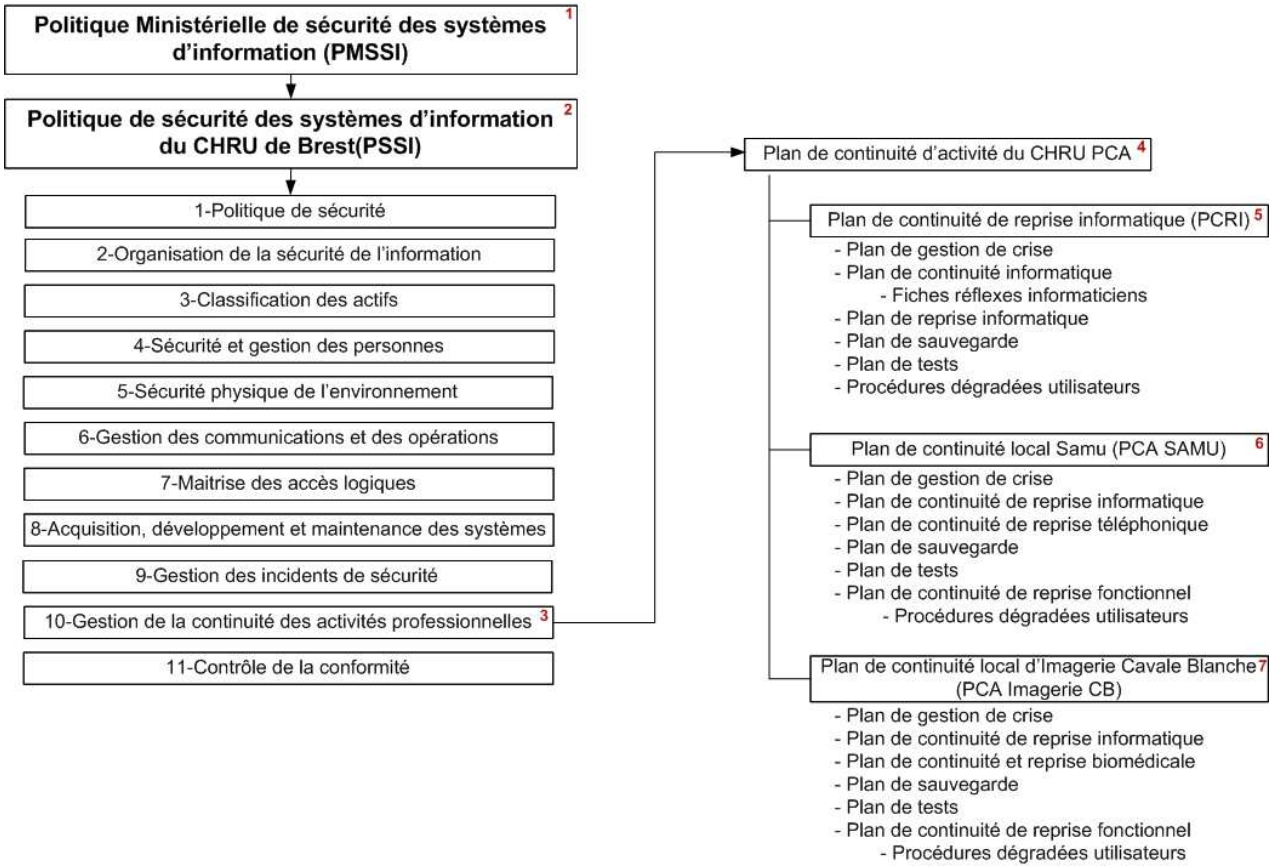


Figure 2 - PMSSI

La PMSSI est réalisée sur la base des normes internationales la série ISO27000 : 27001 pour le management et 27002 pour les bonnes pratiques.

Il n'existe pas aujourd'hui de plan de continuité d'activité PCA au CHRU [**4**] de Brest. Le CHRU de Brest peut être amené à être un acteur majeur lors d'un plan ORSEC, un Plan Grippe, ou encore un Plan Blanc. Ces différents plans sont mis en œuvre lors de sinistres ou catastrophes arrivant en dehors des murs de l'hôpital. Il n'y a ce jour aucun plan de continuité d'activité [**4**] couvrant l'ensemble du périmètre de l'hôpital et qui serait piloté au niveau de la direction générale lors de la survenance d'un désastre majeur au sein des structures de l'hôpital.

De par mes nouvelles fonctions, je suis chargé de piloter la mise en place de la PSSI [**2**] du CHRU de Brest. Le chapitre 10 « Gestion de la continuité des activités professionnelles »[**3**] est un point important de cette PSSI.

Ma proposition initiale de sujet de mémoire est l'étude et la mise en place d'un plan de continuité informatique (PCRI) (**5**). Ce plan comme son nom l'indique a un périmètre restreint à l'informatique et n'est qu'une partie du PCA de l'établissement.

L'activité du SAMU ayant rencontré des perturbations en terme de continuité de service en juillet août 2010, ma direction a souhaité que je pilote et mette en place un plan de continuité spécifique à la mission du SAMU et cela de façon prioritaire. (Plan de continuité local SAMU)(**6**).

Afin de me confronter aux problématiques liées à mes missions futures, ma direction a souhaité que je pilote la mise en place d'un plan de continuité local « Imagerie » à la Cavale Blanche. En effet une nouvelle IRM va être prochainement achetée à l'hôpital de la cavale blanche, la mise en place d'un plan de continuité dans ce service est pour moi l'occasion de prendre en compte les problématiques de sécurité liées à l'intégration d'éléments médicaux gérés par le service biomédical et pleinement interconnectés au système d'information de l'hôpital.

2.4 LES ENJEUX

L'enjeu de ce projet est d'initialiser et mettre en œuvre une démarche de continuité des missions de l'hôpital de manière organisée et formalisée. Cette démarche est soutenue par les directions de l'hôpital au quotidien. Elle doit minimiser l'impact de sinistres majeurs mais également des incidents de sécurité pouvant survenir.

3. ETAT DE L'ART

« On me demande souvent quel conseil je donnerais, qui serait plus utile au monde de l'entreprise, si je devais en donner qu'un. Ma réponse est : un plan de continuité d'activité, simple mais efficace, à jour et régulièrement testé » (Eliza Mannigham-Buller, directrice générale du MI5, novembre 2004, conférence du Confederation of British Industry)

Avec un climat mondial plombé par l'augmentation des sinistres majeurs (en fréquence et en gravité) : tempête dévastatrice de décembre 1999, les attentats du World Trade Center, l'explosion de l'usine AZF de Toulouse en 2001, les inondations du Gard en septembre 2002, les attentats de Madrid en 2004, le tsunami du Sud-Est asiatique en décembre 2004, les attentats de Londres en 2005, le tremblement de terre du Sichuan en 2008, la neige à Marseille et en Provence en janvier 2009, le tremblement de terre de l'Aquila en Italie, le tsunami au Japon en mars 2011, les dirigeants d'entreprises et leurs partenaires sont de plus en plus sensibles aux menaces potentielles qui pèsent sur leur entreprise. Si l'on ajoute à cela, une complexité croissante des organisations (la défaillance d'une entreprise à des effets de bords sur d'autres entreprises ex : la crise de surprime), une dépendance toujours plus forte des entreprises vis-à-vis de leur SI, un durcissement des réglementations concernant la continuité d'activité, une augmentation sensible des exigences clients, les chefs d'entreprises prennent de plus en plus conscience de la nécessité d'un plan de continuité.

Dans ce chapitre, j'expose dans une première partie les grands principes du plan de continuité et les terminologies associées. Puis, j'indique les cadres normatifs et réglementaires existants sur les plans de continuité. Enfin, je décline les étapes permettant la mise en place d'un plan de continuité.

3.1 PRINCIPE D'UN PLAN DE CONTINUITE ACTIVITE

Un PCA Plan de Continuité d'Activité est un dispositif organisationnel et technique qui vise à limiter l'impact potentiel d'un sinistre. Le PCA d'une entreprise n'a pas vocation à répondre à des incidents d'exploitation ou de fonctionnement isolés, le PCA est la solution de la dernière chance, lorsque toutes les protections, les mesures de prévention ont failli et qu'un sinistre a touché le cœur de l'entreprise. Selon la taille de l'entreprise, le plan de continuité peut contenir plusieurs plans locaux propres à des services ou départements particulier de l'entreprise. Le périmètre du PCA couvre toute fonction de l'entreprise qui a pour mission de garantir la sécurité et la continuité des opérations métiers.

Figure 3 - PCA

Ce plan doit permettre de minimiser l'impact d'un sinistre sur l'activité de l'entreprise, assurer le fonctionnement des activités critiques pendant la crise et enfin permettre un retour maîtrisé à une situation d'avant crise.

Pour beaucoup d'entreprises le plan de reprise d'activité se limite à la reprise d'activité informatique PCRI. Elles ne comprennent pas la nécessité d'une prise en compte beaucoup plus globale de la notion de secours. Un PCA couvre la liste non exhaustive des risques et domaines suivant :

- Santé et sécurité du personnel
- Sécurité des produits et santé des clients
- Responsabilité environnementale
- Impact sur l'image, la réputation, les marques
- Perte de compétences et/ou de savoir faire
- Menaces terroristes et conflits militaires
- Destruction de site
- Catastrophes naturelles
- Pertes de réseaux de télécommunications
- Pertes d'infrastructure du SI

« Lorsqu'elles n'y sont pas préparées 43% des entreprises ferment au moment d'un sinistre majeur, et 29% de celles qui survivent périclitent dans les deux ans qui suivent » (Disaster Recovery Institue Internional, Canada, 2001)

Le dispositif d'un PCA s'articule autour de 4 piliers fondamentaux:

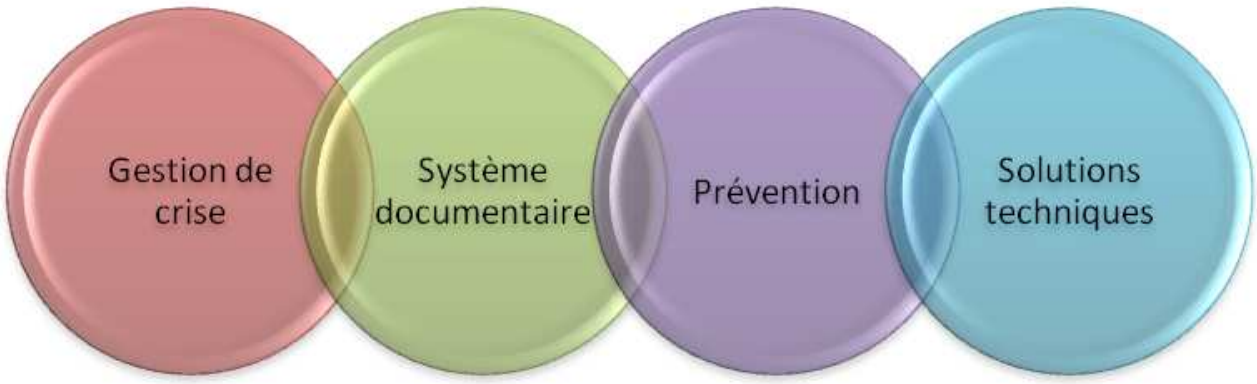


Figure 4 – piliers fondamentaux d'un PCA

Gestion de Crise

L'organisation de gestion de crise assure le bon déroulement du plan de continuité. Le management de la crise et donc le pilotage du déroulement du plan de continuité est avant tout une affaire de décisions et de coordinations.

Système documentaire

Un plan de continuité est un système documentaire, celui-ci doit être éprouvé et à jour. Le système documentaire PCA, devra bien entendu rester disponible après survenance du sinistre.

Prévention

La prévention est l'ensemble des mesures destinées à prévenir des risques (contrôles des accès aux locaux, maintenance préventive des éléments actifs ….) et à réduire l'exposition aux évènements redoutés. L'information des risques auprès du personnel et la sensibilisation de l'ensemble du personnel au plan de continuité est indispensable.

Solutions techniques

Les solutions doivent être pensées pour impacter le moins possible d'utilisateurs après survenance du sinistre. Ces solutions doivent être testées régulièrement.

3.2 QUELQUES DEFINITIONS

« Le PCA constitue l'organisation, les moyens et la formation des modes de réaction de l'organisation aux situations extrêmes auxquelles celle-ci peut être confrontée. » (Plan de continuité d'activité et système d'information vers l'entreprise résiliente, de Matthieu Bennasar)

« Le plan de continuité de service est l'ensemble des mesures visant à assurer, selon divers scénarii de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé des prestations, des services essentiels de l'entreprise puis la reprise planifiée des activités » (Comité de la réglementation bancaire et financière, février 2004)

« Plan de continuité de l'activité : ensemble de mesures visant à assurer, selon divers scénarii de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentiels de l'entreprise puis la reprise planifiée des activités » (CRBF 2004-02)

3.3 TERMINOLOGIES ET VOCABULAIRES

3.3.1 TERMINOLOGIES

Ci-dessus une liste non exhaustive des définitions que l'on peut trouver auprés d'organismes tels que ITIL et le Clusif ou des sociétés de conseil.

- PCA : Plan de Continuité d'Activité (BCP Business Continuity Plan)
- PCO, PCF, PCE : Plan de Continuité d'Opérations, Plan de Continuité Fonctionnelle, Plan de continuité d'exploitation
- PRA : Plan de Reprise d'Activité (DRP Disaster Recovery Plan)
- PSI : Plan de Secours Informatiques (ITCP : IT Contingency Plan)
- PCAI, PCSI, PCRI: Plan de Continuité d'Activité Informatique, Plan de Continuité du Système Informatique, Plan de Continuité et Reprise Informatique, il s'agit du même concept que le PSI
- PGC : Plan de Gestion de Crise (CMP Crisis Management Plan)
- PCM : Plan de Continuité Métiers
- PRAp : Plan de Reprise d'Application

3.3.2 DEFINITION DU VOCABULAIRE

Il est difficile de s'y retrouver tant il existe de définitions et d'acronymes pour définir les composants d'un Plan de Continuité d'Activité. C'est pourquoi il me semble important de faire le point sur les différentes terminologies existantes et de les définir.

Le PCA contient une procédure de gestion de crise et se constitue de 3 plans principaux d'instincts :

Plan de Gestion de crise (PGC) : Ce plan assure la gestion d'une crise, il facilite la coordination et la communication entre toutes les parties impactées (interne et externe à l'entreprise). Il prend en compte la protection du personnel. Ce plan peut contenir les procédures de management de crise (PMC) mais également des procédures d'urgences (PU) et les procédures de relocalisations (PR).

Plan de continuité opérationnel (PCO) : Ce plan fixe les modes opératoires à mettre en œuvre pour assurer la continuité ou la reprise des opérations métiers, en fonction des objectifs opérationnels qui ont été fixés (fonctionnement dégradé des activités jugées critiques).Il regroupe les Procédures Fonctionnelles de Continuité (PFC).

Le plan de continuité et reprise du système d'informatique (PCRI) : Ce plan définit les modes opératoires à respecter pour assurer la continuité ou la reprise des systèmes informatiques. Le PCRI définit également les moyens à mettre en œuvre, comme le site de backup ou les technologies employées.

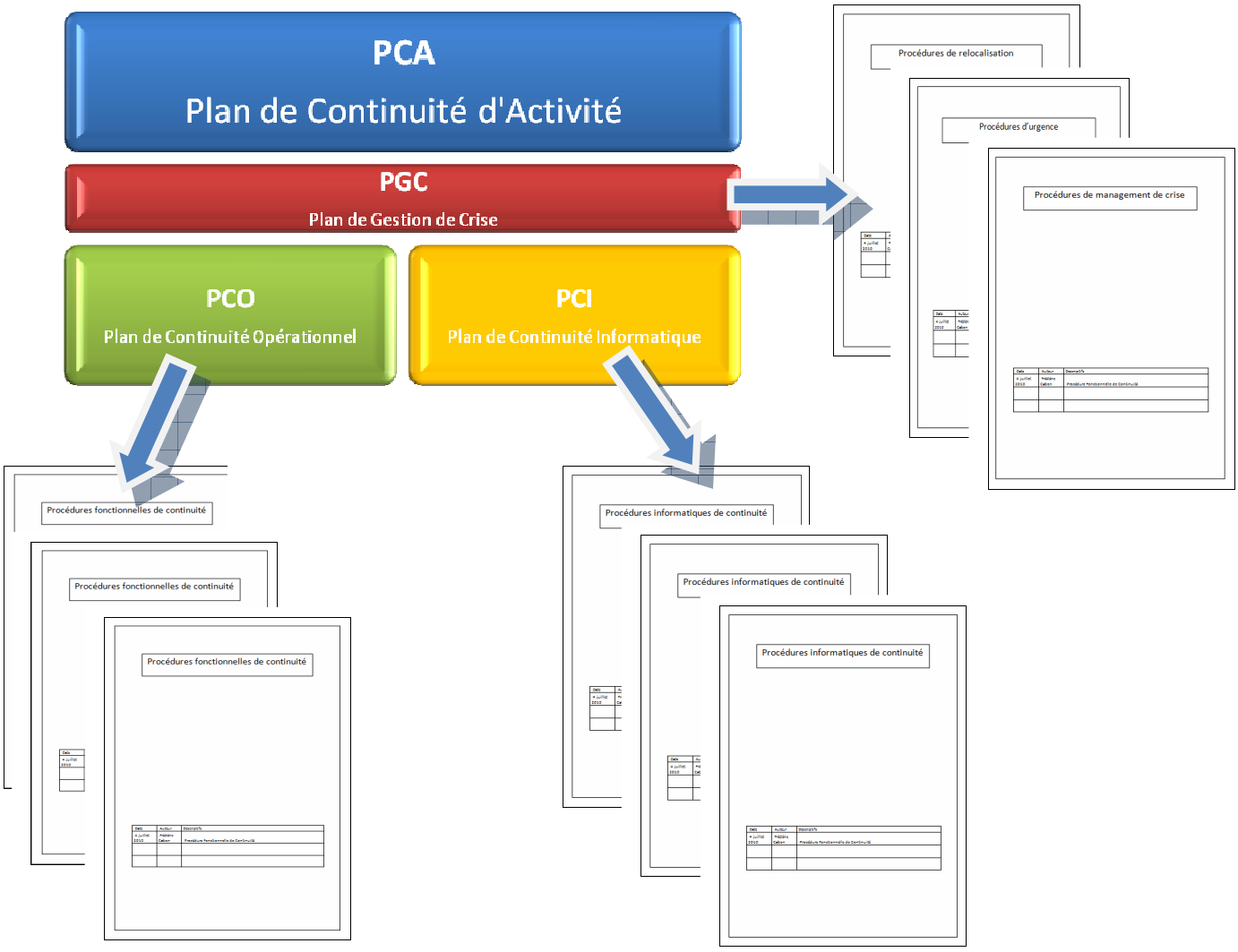


Figure 5 - exemple de contenu d'un PCA

3.3.3 AUTRES TERMINOLOGIES

Risque = (Menace x Vulnérabilité) / contre mesure

Risque : Perte potentielle, identifiée et quantifiable (enjeux), inhérente à une situation ou une activité, associée à la probabilité de l'occurrence d'un événement ou d'une série d'événements.

Menace : Une menace est la cause potentielle d'un ou plusieurs incidents. Et peut résulter en un dommage au système ou à l'organisation (définition selon la norme de sécurité des systèmes d'information ISO 13335-1).

Vulnérabilité : Faiblesse dans un système ou une organisation permettant à un attaquant de porter atteinte à son intégrité ou à son fonctionnement normal.

Contre mesure : solutions techniques (de type cluster), sensibilisation

Impact : C'est une mesure des effets tangibles et intangibles, positifs et négatifs qu'un incident, un accident, un changement, un problème ou un mouvement a, ou pourrait avoir, sur son environnement.

Priorité : C'est l'ordre dans lequel un incident, un problème, un risque doivent être traités.

3.4 CADRE NORMATIF ET REGLEMENTAIRE

Plusieurs normes, méthodes et référentiels de bonnes pratiques en matière de sécurité des systèmes d'information et continuités d'activité existent. Elles constituent des guides méthodologiques ainsi que le moyen de fournir l'assurance d'une démarche de sécurité cohérente.

La plupart des textes réglementaires relatifs aux activités commerciales et financières imposent des exigences de maîtrise des risques et de contrôle interne qui touchent plus ou moins directement la continuité d'activité. Voici une liste des principales réglementations et normes traitant de la continuité d'activité.

3.4.1 LES REGLEMENTATIONS

Bâle II : La réglementation Bâle II (le Nouvel Accord de Bâle) constitue un dispositif destiné à mieux appréhender les risques bancaires et principalement le risque de crédit ou de contrepartie et les exigences en fonds propres.

Le comité de Bâle sur le contrôle bancaire, fondé en 1975 et regroupant les gouverneurs de banques centrales des pays du G10 publie un ensemble de recommandations dont le pivot est la mise en place d'un ratio minimal de fonds propres par rapport à l'ensemble des crédits accordés, le ratio Cooke. Ainsi sont définies les notions de : fonds propres réglementaires et d'ensemble des engagements de crédit.

La nouveauté de Bâle II est l'ajout aux risques classiques de crédit et de marché la prise en compte d'un risque opérationnel : le ratio de Mc Donought. Selon la définition de Bâle II, le risque opérationnel est un « risque de pertes résultant de procédures internes inadéquates ou défaillantes, des personnels, des systèmes ou d'événements extérieurs. » Cet accord inclut pleinement les risques du SI liés à la problématique continuité d'activité.

http://www.bis.org/bcbs/index.htm

Loi n°2003-706 du 1er aout 2003 sur la sécurité financière : Cette loi précise des exigences fortes en terme des procédures de contrôle interne et donc de la continuité d'activité.

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000428977

L'Instruction générale interministérielle relative à la sécurité des activités d'importance vitale : Cette instruction regroupe les plans ORSEC, VIGIPIRATE et définit un cadre de maîtrise des risques et de continuité d'activité pour les biens et les services considérés d'importance vitale pour la France.

« Les plans de continuité d'activité visent à assurer le fonctionnement des activités essentielles des administrations et des opérateurs et la disponibilité des ressources indispensables au déroulement de leurs activités. Ils doivent par conséquent permettre notamment la poursuite des activités au sein des points d'importance vitale auxquels ils se rapportent.

Le dispositif de sécurité des activités d'importance vitale et les plans de continuité d'activité s'intègrent dans une même logique de gestion de crise. Ils doivent être parfaitement compatibles entre eux et tendre vers les mêmes objectifs de continuité de l'activité et de sauvegarde de la ressource. » Extrait du chapitre 1.3.5

http://www.circulaires.gouv.fr/pdf/2009/04/cir_1338.pdf

CIRCULAIRE DGT 2007/18 du 18 décembre 2007 relative à la continuité de l'activité des entreprises et aux conditions de travail et d'emploi des salariés du secteur privé en cas de pandémie grippale :

« Il est fortement recommandé à chaque chef d'entreprise de formaliser l'ensemble des mesures internes à l'entreprise qui auront été préparées, en amont d'une pandémie grippale, dans un « plan de continuité », régulièrement actualisé en fonction de l'évolution de la situation qui sera indiquée par les autorités publiques. » Extrait du chapitre 2.2

Cette circulaire définit un cadre de travail pour le salarié en cas de pandémie, il aborde principalement la prévention, le droit de retrait, le travail à distance, la polyvalence des employés.

http://www.circulaires.gouv.fr/pdf/2009/04/cir_2047.pdf

Plan national de prévention et de lutte pandémie grippale (n° 150/SGDN/PSE/PPS du 20 février 2009) : Ce plan propose une démarche d'anticipation afin d'assurer, en cas de pandémie grippale, le fonctionnement du pays dans des conditions aussi normales que possibles (prévention, confinement, réponse sanitaire …).

« La réponse à la pandémie grippale relève donc d'approches intersectorielles très diverses et interdépendantes, à la croisée de planifications liées à d'autres risques de grande ampleur.

Les principaux objectifs du plan sont de protéger la population en métropole et outre-mer, ainsi que les ressortissants français à l'étranger, contre une menace de pandémie grippale. Pour ce faire, le plan vise également à préserver le fonctionnement aussi normal que possible de la société et des activités économiques. »

http://www.pandemie-grippale.gouv.fr/IMG/pdf/PLAN_PG_2009.pdf

CRBF 2004-02 : Le CRBF 2004-02 (modifiant le Règlement 97-02) donne en son article 4, la définition du Plan de Continuité d'Activité « ensemble de mesures visant à assurer, selon divers scénarii de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités. " En outre, l'article 14-1 dudit règlement 2004-02 dispose que « les entreprises assujetties doivent :

A- Disposer de plans de continuité de l'activité

B- S'assurer que leur organisation et la disponibilité de leurs ressources humaines, immobilières, techniques et financières font l'objet d'une appréciation régulière au regard des risques liés à la continuité de l'activité

C- S'assurer de la cohérence et de l'efficacité des plans de continuité de l'activité dans le cadre d'un plan global qui intègre les objectifs définis par l'organe exécutif et, le cas échéant, par l'organe délibérant »

http://www.pwc.fr/fr/pwc_pdf/pwc_controle_interne.pdf

3.4.2 LES NORMES ET STANDARDS

BS25999 : Cette norme fait suite aux travaux du BCI(1). La norme BS 25999 a été conçue par un grand groupe d'experts mondiaux représentatif de divers secteurs d'activité et par le gouvernement pour établir les processus, les principes et la terminologie liés à la gestion de la continuité des activités

Elle est déclinée logiquement sous deux aspects :

BS 25999-1 (Code de bonne pratique) offre les recommandations pour les meilleures pratiques de GCA. Il faut noter que celle-ci n'est qu'un document guide.

BS 25999-2 (Les Spécifications) fournit les exigences requises pour un Système de Gestion de la Continuité des Affaires (SGCA) basé sur les meilleures pratiques de la GCA. Cette partie de la norme peut être utilisée pour démontrer la conformité par le biais d'un audit et du processus de certification. Cette norme propose une démarche de management organisée en 5 étapes

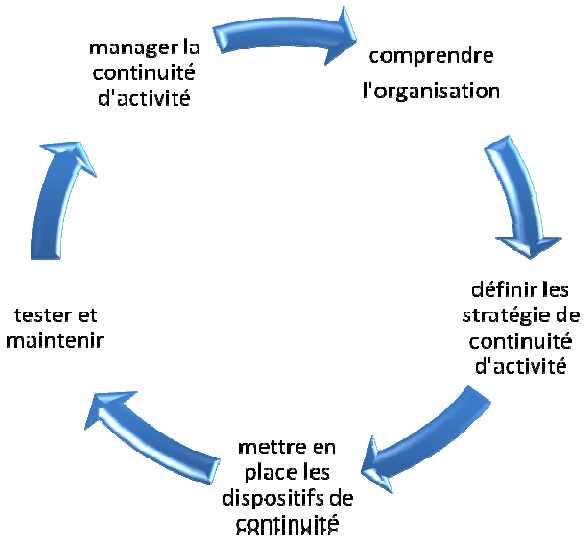


Figure 6– étapes BS25999

http://www.bsigroup.ca/fr-ca/audit-et-certification/systemes-de-gestion/normes-et-programmes/bs25999/

BP Z74-700 : Publié en 2006 par Afnor (Association française de normalisation) ont été élaborées des bonnes pratiques en matière de plan de continuité de services et de reprise des activités des systèmes d'information. Ce travail d'harmonisation s'est appuyé sur des documents déjà existants comme par exemple des chartes développées au sein des entreprises et les travaux de recherche en la matière. Le groupe de travail a contribué également à la définition d'une norme internationale. Il continuera à apporter le point de vue issu d'une réflexion nationale.

Ce référentiel contient 5 grands thèmes :

- Remontées d'incidents, évaluation et alerte
- Cellule de gestion de crise
- Plan de continuité des opérations
- Plan de continuité informatique et télécoms
- Maintenance en condition opérationnelle

Ce code de bonne conduite met l'accent sur le facteur humain en y consacrant un chapitre, éléments que les autres normes ont tendance à passer sous silence

La norme ISO/CEI 27001 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information.

http://portailgroupe.afnor.fr/public_espacenormalisation/AFNORGCSECU/r%C3%A9union%20d%27information.pdf

ISO 27002 : ce référentiel est plus un code de pratique, qu'une véritable norme ou qu'une spécification formelle telle que l'ISO 27001. Elle présente une série de contrôles (39 objectifs de contrôle) qui suggèrent de tenir compte des risques de sécurité des informations relatives à la confidentialité, l'intégrité et les aspects de disponibilité. Les entreprises qui adoptent l'ISO/CEI 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés, en utilisant la norme pour orienter l'entreprise.

Le chapitre 14 de l'iso 27002 traite tout particulièrement de la gestion du plan de continuité de l'activité :

- 14. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité
- 14.1 Intégration de la sécurité de l'information dans le processus de PCA
- 14.2 Continuité de l'activité et appréciation du risque
- 14.3 Elaboration et mise en œuvre des PCA intégration la sécurité de l'information
- 14.4 Cadre de la planification de la continuité de l'activité
- 14.5 Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité

Le référentiel ISO 27002 présente la continuité d'activité comme un des maillons de la gestion de la sécurité de l'information.

http://www.27000.org/iso-27002.htm

ARCHITECTURE DE LA NORME ISO 27001

La norme ISO 27002 est structurée en 11 chapitres, visant 39 objectifs de sécurité et identifiant 133 règles. L'ensemble de ces règles couvre le champ de la sécurité des systèmes d'information pour atteindre le niveau adéquat visé par l'organisme. Cette norme fournit des recommandations de gestion de la Sécurité de l'information au RSSI pour initier, implémenter et maintenir la sécurité.

Figure7 - Extraite de la Page 28 de la PMSSI Politique Ministérielle de Sécurité des Système d'Information

Le standard international ITIL(1): ITIL est un ensemble d'ouvrages recensant les bonnes pratiques ("*best* practices") pour la gestion des services informatiques, dicté par l'Office public britannique du Commerce (OGC). L'adoption des bonnes pratiques de l'ITIL par une entreprise permet d'assurer à ses clients un service répondant à des normes de qualité pré-établies au niveau international. ITIL est à la base de la norme BS15000 un label de qualité proche des normes de l'ISO (Organisation internationale de normalisation).

ITIL permet, grâce à une approche par processus clairement définie et contrôlée, d'améliorer la qualité des SI et du support aux utilisateurs en créant notamment la fonction de Centre de services ou « Service Desk » centralise et administre l'ensemble de la gestion des systèmes d'informations. ITIL peut être considéré comme un "règlement intérieur" du département informatique des entreprises qui l'adoptent.

Les bénéfices pour l'entreprise sont une meilleure traçabilité de l'ensemble des actions du département informatique. Ce suivi amélioré permet d'optimiser en permanence les processus des services pour atteindre un niveau de qualité maximum de satisfactions des clients.

La section 7 du référentiel ITIL « IT Service Continuity Management » encadre la continuité de service.

Chapitre du « IT Service Continuity Management » :

- 1. Périmètre et risques couverts
- 2. Cycle de vie de la continuité des activités métiers
- 4. Etape 1 : Initialisation
- 5. Etape 2 : Besoins et stratégie
- 6. Etape 3 : Implantation
- 7. Etape 4 : Gestion opérationnelle
- 8. Déclenchement
- 9. Projet de mise en œuvre de la continuité

http://www.itilfrance.com/index.php?pc=pages/docs/itilv2/21-5-index_cont.inc&pg=menu_itilv2.inc&pt=La%20gestion%20de%20la%20continuit%E9%20de%20service

3.5 ACTEURS ET ACTIVATION DU PCA

3.5.1 LES ACTEURS

Les acteurs d'un PCA sont des personnes capables de garantir un ensemble de tâches de pilotage ou de mise en œuvre des moyens de secours. Les premiers intervenants doivent donner l'alerte selon la procédure d'escalade définie.
Lors d'un sinistre les entités suivantes se formeront :
Cellule de crise
Comité de coordination
Equipe d'intervention
Référents utilisateurs

3.5.2 CELLULE DE CRISE

La cellule de crise prend les décisions, elle analyse le contexte et décide le déclenchement de telle ou telle action. Cette cellule peut être composée par les membres la direction générale, les directions des services généraux, la direction du système d'information, la direction des communications, des directions juridiques, le responsable du plan de continuité. Des moyens de communications préétablis sont mis en œuvre tels que des salles de réunion, une liste des numéros téléphone, d'email.

3.5.3 COMITE DE COORDINATION

Le comité de coordination vient en suppléant de la cellule de crise, il s'occupe de la logistique et de la coordination des actions décidées par la cellule de crise. Il est directement en contact avec les équipes d'intervention, mais aussi communique avec les référents métiers. Cette équipe, comprend des personnes de l'entreprise ayant une maitrise du plan de continuité et peut être piloté par le responsable du plan de continuité.

3.5.4 EQUIPE D'INTERVENTION

Cette équipe regroupe l'ensemble des personnes ayant les compétences requises pour réaliser les taches de secours ou de remise en services des éléments actifs. Il peut s'agir d'ingénieurs ou techniciens réseaux, SAN, administrateurs serveurs ou poste de travail. Certains de ces acteurs peuvent être externes à l'entreprise (prestataires, fournisseurs, opérateurs …), ils doivent être clairement identifiés. Une liste des coordonnées de l'ensemble de ces acteurs internes et externes est tenue à jour.

3.5.5 REFERENTS UTILISATEURS

Les référents utilisateurs se composent de personnes « métiers ». Ils ont en charge de faire appliquer les procédures dégradées à la survenance d'une panne ou d'une crise. Ces référents seront en contact avec la cellule de coordination et devront appliquer les procédures de reprise lors de la fin de crise et donc du retour à la normale.

3.5.6 ALERTE ET ACTIVATION DU PCA

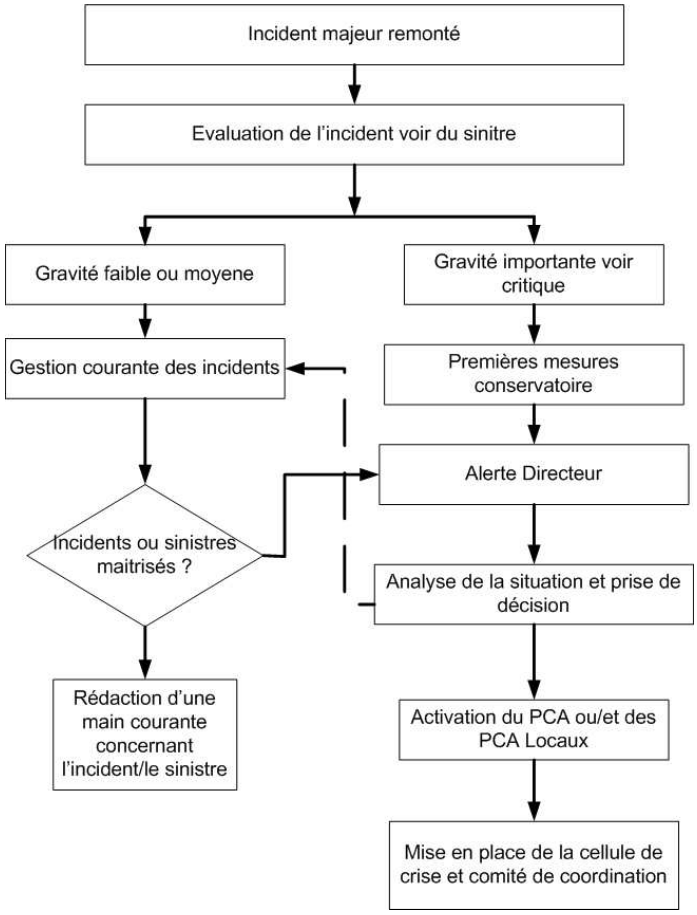


Figure 7 - logigramme alerte et activation du PCA

3.6 LES PHASES DE LA DEMARCHE PCA

Dans ce chapitre je décris les différentes phases nécessaires à la mise en place et au déploiement d'un plan de continuité d'activité.

Un des postulats à la mise en place d'une démarche d'envergure tel qu'un PCA, est le soutien du projet au plus haut niveau hiérarchique possible de l'entreprise.

Au vu des sommes et de la charge de travail engagée lors de la mise en place d'une démarche de continuité d'activité, il est indispensable de définir une stratégie de secours adaptée aux enjeux et contraintes de l'entreprise. Avant de commencer une telle étude, il convient de faire valider par la direction générale, via un comité de pilotage les activités de l'entreprise concernées et les types de risques à prendre en charge. Il peut s'agir de l'ensemble des activités ou au contraire de plans « locaux » limités à un service ou un domaine stratégique particulier. Selon les risques retenus et le périmètre souhaité, le plan élaboré sera un plan de continuité informatique ou s'apparentera à un plan de continuité d'activité pouvant comprendre plusieurs plans locaux

différents. Pour les hôpitaux la classification des risques prendra en compte les impacts sur la santé du patient et l'image de l'établissement bien avant les possibles impacts financiers.

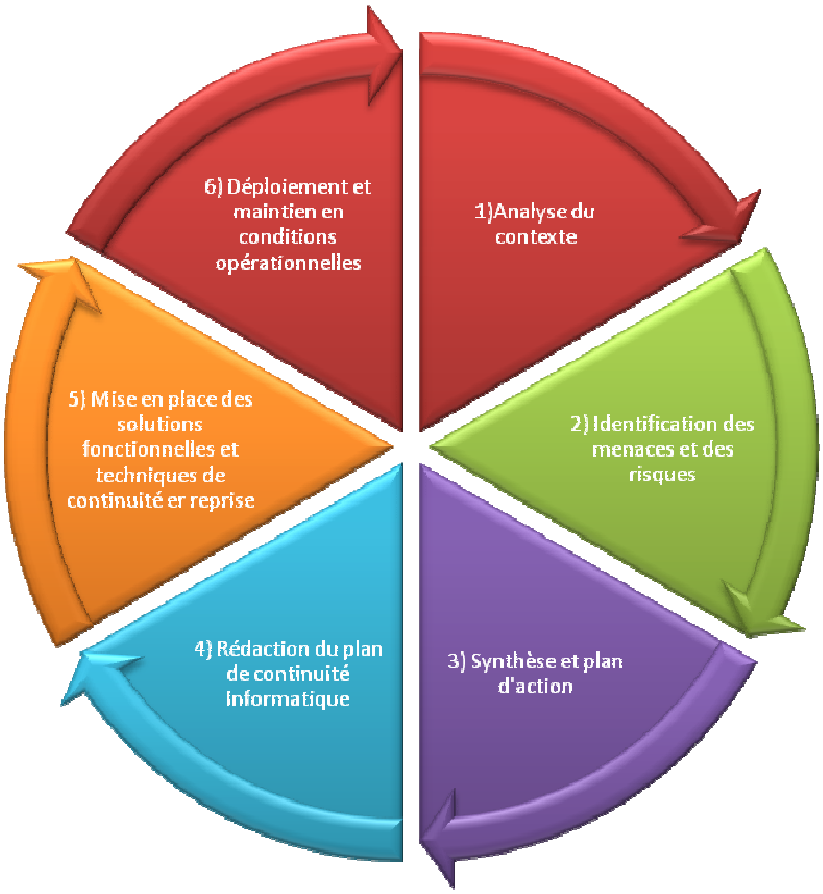


Figure 8 - phases de la démarche PCA

3.6.1 PHASE 1 – LANCEMENT, ORGANISATION CONDUITE DU PROJET

Dans cette phase on détermine les bases du projet, à savoir la composition de l'instance de pilotage, des équipes projets. L'objectif et le périmètre fonctionnel sont clairement établis. Un planning précis des taches est définit.

Les phases 2 et 3 sont des phases de spécifications fonctionnelles qui délimitent les périmètres et les contours des solutions de continuité organisationnelles et techniques.

3.6.2 PHASE 2 – ANALYSE DU CONTEXTE ET CARTOGRAPHIE DU SI

Dans cette phase, il convient de collecter tous les éléments nécessaires à l'analyse du projet, en réalisant l'inventaire des processus métiers, puis de les détailler, et de réaliser un relevé des actifs (outils, logiciels, matériels, infrastructures, sites d'établissement …). Une cartographie des processus métiers et du système d'information peut être entreprise.

3.6.3 PHASE 3 – IDENTIFICATION DE MENACES ET DES RISQUES

Cette phase comprend deux étapes majeures, à savoir l'analyse des risques et l'inventaire des besoins en terme de continuité.

Etape 1 Analyse de risque

L'objectif de cette étape est de cartographier les sinistres contre lesquels l'entreprise cherchera à se prémunir. Pour ce faire, dans un premier temps on cherchera à dresser un panorama si possible exhaustif des menaces qui pèsent sur l'entreprise. Ces menaces et vulnérabilités peuvent être d'ordre varié:

- organisationnelles (Pandémie …)
- opérationnelles
- techniques
- sécuritaires

Dans un second temps, on dessine la cartographie des risques. Le but est d'évaluer pour chaque menace la probabilité d'occurrence et l'impact potentiel de la menace sur les processus jugés critiques.

Pour ce faire, les risques sont catégorisés et regroupés en scénarii selon leur type et leur impact potentiel.

L'évaluation du risque se fera selon 2 critères : L'impact et la probabilité que le risque survienne

Au terme de cette étape, une cartographie des sinistres ainsi que les scénarii de sinistres retenus doivent être livrés.

L'une des méthodes la plus complète est sans nul doute l'analyse des risques EBIOS (Expression des besoins et indentification des objectifs de sécurité). Celle-ci est une méthode très complète qui permet d'aborder de façon systématique l'analyse des risques et des vulnérabilités des systèmes d'information. D'autres outils et guides pratiques sont mis à disposition gratuitement et peuvent aider à réaliser la cartographie des risques. On citera notamment les méthodes Marion ou Méhari du Clusif (Club de la sécurité des systèmes d'information français).

<u>Etape 2</u> Inventaire des besoins en continuité

« La principale difficulté d'un plan de reprise d'activité n'est pas tant d'implémenter une solution technique que de mener une analyse d'impact méthodique, de délimiter précisément le périmètre applicatif concerné, et de définir la nature des besoins » extrait de l'article reprise d'activité : n'oubliez pas le backup écrit par Thierry Jacquot et publier dans le magazine 01 Informatique.

L'objectif de cette étape est d'étudier l'ensemble des processus et leurs besoins en continuité et d'estimer les durées d'interruption maximales admissibles (et raisonnables) les DIMA. On identifiera également des ressources clés liées à chaque activité, ceci permettra de déterminer au mieux les modes dégradés de fonctionnement.

Pour récolter ces informations, des colloques ou réunions peuvent être organisées.

Les données de sortie sont les indicateurs de sécurité RTO et RPO.

Le RTO pour « Recovery Point Objective », désigne la durée maximale d'interruption admissible vis-à-vis de l'utilisateur métier, c'est-à-dire le temps maximal acceptable, pendant lequel une ressource informatique n'est plus fonctionnelle.

Le RPO « Recovery Time Objective », est la durée maximale d'enregistrement des données qu'il est acceptable de perdre. Cet indicateur permet de juger au mieux des sauvegardes à mettre en œuvre.

3.6.4 PHASE 4 – SYNTHESE ET PLAN D'ACTION

Selon les résultats de l'analyse menée dans la phase 3, on dressera la liste des actions à effectuer pour la réduction des risques. On tachera de prioriser le traitement des risques, et l'on proposera des solutions et contremesures pouvant être des méthodes d'ordre organisationnel et des moyens techniques.

Les solutions techniques et méthodes sont à déterminer avec les experts techniques de l'entreprise et les responsables fonctionnels, puis validées par le comité de pilotage.

Des préconisations sur les solutions sont clairement établies et les cahiers des charges des solutions techniques sont rédigés.

3.6.5 PHASE 5 – ELABORATION DES PLANS DE CONTINUITE

Selon la taille, la typologie, les activités de l'entreprise et sa maturité vis-à-vis de la continuité d'activité, le contenu du PCA sera plus ou moins important. On pourra retrouver les plans suivants :

<u>Plan de gestion de crise</u>

Ce document décrit l'ensemble des acteurs et décrit leurs responsabilités. Il décrit la mise en œuvre de la cellule de crise et la gestion opérationnelle de la crise.

Il comprend le synoptique de la gestion de crise, de la survenance du sinistre au retour fonctionnel et technique initial.

Procédures d'urgence

Ces directives décrivent d'une manière simple les premières réactions que doivent avoir les employés lors de la survenance d'un sinistre. On y indiquera les numéros des services d'urgences comme les pompiers, le SAMU, et les services internes à prévenir.

Plan de continuité et de reprise informatique

Ce document décrit l'architecture informatique, et les mesures techniques de secours mises en œuvre pour assurer la continuité informatique des applications métiers.

Ce plan contient en annexe, les procédures de continuité informatique, autrement appelées fiches réflexes informatiques.

Plan de sauvegarde

Ce document décrit les processus de sauvegarde mis en œuvre pour assurer les sauvegardes des données. Il contient également les procédures de restauration de chaque type de donnée sauvegardée.

Plan de test

Des tests de continuité sont régulièrement effectués (Ref : chapitre 3.6.7 Phase 7 – Déploiement et maintien en conditions opérationnelles). Un planning des tests effectués est tenu à jour. Les scénarii de tests et les rapports de ceux-ci sont ajoutés en annexe.

Plan de continuité et de reprise fonctionnel

Ce document décrit les mesures à mettre en œuvre à la survenance d'une panne, quelle que soit l'origine. En annexe de ce plan, on retrouvera les procédures dégradées utilisateurs et fiches réflexes utilisateurs.

3.6.6 PHASE 6 – MISE EN PLACE DES SOLUTIONS FONCTIONNELLES ET TECHNIQUES DE CONTINUITE

Les solutions fonctionnelles de continuité, aussi appelées procédures dégradées, sont rédigées en collaboration avec les personnes du métier, celles-ci doivent être testées régulièrement. Elles décrivent le fonctionnement de l'activité en mode dégradé, c'est-à-dire lors du disfonctionnement total ou partiel de SI. En plus de la définition du mode dégradé, elles peuvent également décrire les modalités du retour à la normale.

Les spécifications des solutions techniques ont été définies lors de la phase 4, il s'agit donc ici de mettre en œuvre les solutions techniques en mode projet : composition des équipes projet, mise en place d'un planning de déploiement.

Des tests de validation fonctionnels et techniques doivent être réalisés après l'installation d'un élément majeur dans l'infrastructure.

3.6.7 PHASE 7 – DEPLOIEMENT ET MAINTIEN EN CONDITIONS OPERATIONNELLES

Dans la phase de déploiement, la sensibilisation, la formation et surtout la communication sur le PCA est un élément indispensable et à ne surtout pas négliger. Il faut s'assurer que la PCA soit connu de tous et reste opérationnel malgré les changements et évolution interne de l'entreprise. Dans cette phase on retrouve deux étapes majeures. La première étape, consiste à définir les conditions à mettre en œuvre pour maintenir le plan à jour et opérationnel, puis dans un second temps réaliser les opérations de maintien. Pour s'assurer que le PCA est efficace dans le temps, il convient de définir des tests de PCA à effectuer de façon périodique. Ces tests permettent de déceler les insuffisances ou les défaillances du dispositif de continuité.

Il y a possibilité de réaliser des tests « théoriques » donc sur papier et autour d'une table, ce type de test est simple à mettre en œuvre, peu coûteux et n'a pas d'impact sur la production. Les tests « réels » sont évidement plus probants mais plus difficiles à mettre en œuvre, car plus coûteux en temps, en ressources humaines et a un impact sur la production.

4. ETUDE DE CAS : MISE EN PLACE DE PLANS DE CONTINUITE AU CHRU DE BREST

La mise en œuvre du plan de continuité d'activité du CHRU, est une démarche à long terme. Etant donnés la typologie et le nombre de services constituant l'hôpital, la couverture complète de l'hôpital par la démarche PCA se fera sur plusieurs années.

Ce chapitre décrit la mise en œuvre de 2 plans de continuité :

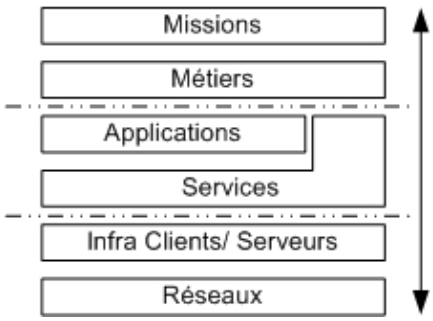
- Plan de continuité et de reprise informatique (PCRI) : Ce plan comme son nom l'indique a un périmètre défini à l'informatique de l'hôpital.
- Plan de continuité local SAMU (PCA SAMU) : L'activité du SAMU ayant rencontré des perturbations en terme de continuité de service en juillet aout 2010, ma direction a souhaité que je pilote et mette en place un plan de continuité spécifique à la mission du SAMU.

Le Plan de continuité local d'Imagerie Cavale Blanche (PCA Imagerie CB) devant se dérouler au second semestre 2011, il ne sera pas traité dans ce chapitre.

La réalisation de chacun des plans s'est réalisée en mode projet. Ainsi un planning et un plan d'actions ont été déterminés pour chacun de ces projets. La démarche PCA décrite dans le chapitre 3.5 est mise en application pour la réalisation de chacun des projets.

Dans ce chapitre je décris la mise en œuvre des 2 projets réalisés lors de mon projet de mémoire d'ingénieur. Chacun de ceux-ci comprend 6 phases projets. La première phase décrit le lancement, l'équipe projet, le périmètre du projet (processus métiers couvert par le plan de continuité). Dans la seconde phase, est décrite l'analyse des risques réalisée. Dans la troisième phase, je décris les contremesures techniques à mettre en œuvre suite aux résultats de l'analyse des risques. La quatrième phase traite des plans de continuités autrement appelés dans un contexte projet les livrables. La cinquième partie montre les solutions fonctionnelles et techniques déployées. Enfin dans la dernière phase, je reviens sur le maintien en condition opérationnel e des solutions mises en place.

Afin d'aider à la lecture du mémoire, un macaron est placé dans certain chapitre. Celui ci doit aider le lecteur à se rendre compte dans quelle « couche » se trouve le chapitre et donc les éléments qui y réfèrent.



Ce macaron se compose de 6 couches distinctes. La couche réseaux et la couche Infra Clients / Serveurs est ce que l'on appelle aussi le « cloud ». Ces couches basses sont des couches purement techniques et matérielles.

Les couches du milieu, sont les couches services et applications. Les services sont les logiciels transverses qui ne sont pas directement liés aux processus métiers tels que les partages de

fichiers, les emails, l'intranet et l'accès au web. Les applications représentent les logiciels métiers utilisés par les personnels de l'hôpital.

Les couches les plus hautes représentent les processus métiers et fonctionnels nécessaires pour assurer les différentes missions du personnel du CHRU. C'est à ce niveau que l'on retrouvera l'ensemble des plans de continuités.

Je n'ai pas choisi le modèle OSI, car je ne le trouvais pas assez représentatif pour définir les éléments PCA.

Récapitulatifs des livrables

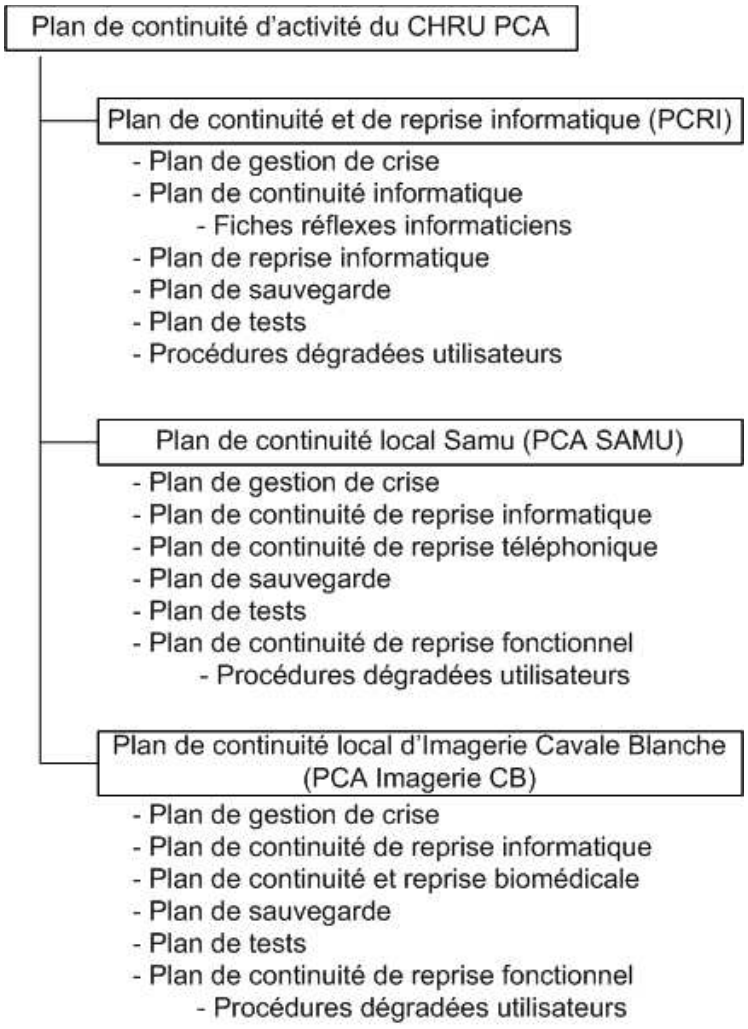


Figure 9 – Phases de la démarche PCA

4.1 PLAN DE CONTINUITE ET DE REPRISE INFORMATIQUE

4.1.1 LANCEMENT, ORGANISATION ET CONDUITE DU PROJET

Dans ce chapitre je définis dans un premier temps le contexte et la démarche de ce projet. Puis je rappelle l'engagement de la direction, le périmètre, et les équipes associées au projet. Enfin je montre le planning et le plan d'actions.

4.1.1.1 DEMARCHE ET OBJECTIF

Le cœur d'activité qui est le soin a fait l'objet d'une couverture dématérialisée de plus en plus étendue au fil du temps. Le système d'information a pris une place importante dans la prise en charge du patient et l'activité de soins.

Cela suppose donc :

- D'assurer la continuité de service et une disponibilité très forte
- D'assurer en cas d'indisponibilité programmée et/ou accidentelle, une continuité à travers la mise en place de procédures dégradées, entretenues au fil du temps, connues des acteurs métiers

4.1.1.2 ENGAGEMENT DE LA DIRECTION

Le projet de Plan de Continuité et de Reprise Informatique a été validé par la direction du système d'information.

« *De manière plus précise le CHRU, se positionne pour élaborer un PCRI, plan de continuité et de reprise d'activité du système informatique, ciblé sur la prise en charge administrative et soignante du patient. Ce plan de continuité d'activité ciblé, contient également le volet professionnel métier, à travers la prise de connaissance des procédures dégradées et à la mise en pratique de celles-ci.*

C'est dans ce cadre que le CHRU de Brest, a positionné un poste de RSSI, placé sous le Directeur informatique, en position transversale, assurant également les fonctions de responsable qualité DSIS. Les deux fonctions RSSI et responsable qualité s'appuyant partiellement sur des normes convergentes ». Extrait de la lettre d'engagement « démarche sécurité niveau régional » rédigée et signée par Monsieur Legeas Directeur de la Direction du Système d'Information du CHRU de Brest en juin 2010.

4.1.1.3 PERIMETRE DU PLAN DE CONTINUITE ET DE REPRISE INFORMATIQUE

Le plan de continuité informatique couvre un périmètre défini en terme de processus métier :

Processus métier

- Identification et localisation des patients
- Gestion des laboratoires
- Dossier patient et processus de Soins
- Gestion des dossiers médicaux
- Gestion des services d'urgences

Les objectifs ont été clairement définis lors de ma présentation à la direction de la DSIS le 25 octobre 2010.

4.1.1.4 COMPOSITION DE L'INSTANCE DE PILOTAGE ET DES EQUIPES PROJETS

Composition de l'instance de pilotage

Une équipe pilote le projet, celle-ci est en charge de valider les choix techniques et organisationnels. Cette équipe suit également le planning.

Cette équipe est composée de :

- Monsieur Legeas, DSI
- Monsieur Madec, Responsable Projet
- Monsieur Pallie,r Responsable Groupe applications métiers
- Monsieur Jacolot, Attaché d'Administration
- Monsieur Jacquemin, Responsable Groupe technologies
- Moi-même en tant que RPCRI (Responsable PCRI)

Composition de l'équipe projet PCRI

Suite à ma prise de fonction en tant que Responsable Sécurité du Système d'Information, j'ai créé un groupe sécurité avec l'accord préalable de ma direction. La première réunion c'est déroulée le 13 janvier 2011, depuis une réunion est planifiée tous les 2emes jeudis du mois. Le groupe de travail « sécurité » se réunit également de façon ponctuelle. J'ai demandé en accord avec la direction de la DSIS, que l'on traite en priorité de la continuité d'activité et donc du projet PCRI, le groupe devant par ailleurs traiter divers points liés à la sécurité du SI.

Ce groupe est animé par moi-même et a comme objectif de:

- Evaluer les incidents de sécurité et émettre des recommandations
- Corrections et axes d'amélioration en termes de continuité de services
- Définir et mettre à jour les processus opérationnels de sécurité : PSSI
- Coordonner la mise en œuvre des mesures de sécurité
- Sensibiliser en matière de sécurité de l'information

Cette équipe est composée de :

- Jean Pierre Pallier, Responsable Groupe applications métiers (GAM)
- Patric Jacquemin, Responsable Groupe technologies (GT)
- Freddy Rosenberg, Ingénieur Projet
- Elodie Guiziou, Ingénieur réseau
- Jean Yves Le Henaff, Ingénieur système
- Patrice Menou, Technicien système micro
- Alexandre Robbe, Technicien système micro
- Gérard Billhant Administrateur base de données (DBA)
- Moi-même en tant que RSSI

En ce qui concerne la rédaction des procédures fonctionnelles et la validation du BIA, les personnels métiers sont mis à contribution selon les processus fonctionnels traités.

4.1.1.5 PLANNING ET PLANS D'ACTIONS

Etat d'avancement au 1er juin 2011 – en vert le réalisé, en jaune en cours de réalisation, en bleu le reste à faire.

Planning et Plan d'action pour la mise en place du PCRI					
			Début	Fin	Etat
Phase	*Fiche de l'action (objet)*	*Objectifs de l'action*			
1 Lancement,organisation et conduite de projet (chap : 4.1.1)	1.1 La démarche	Définition de la démarche	sept-10	sept-10	
	1.2 Engagement de la Direction	Valider le projet de Plan de Continuité et Reprise Informatique	sept-10	sept-10	
	1.3 Périmètre du Plan de Continuité et de reprise informatique	Valider les objectifs, le périmètres, le planning et les moyens alloués à la mise en place du PCRI	25-oct-10	25-oct-10	
	1.4 Composition d'une instance pilotage et de l'équipe projet	Composition de l'instance de pilotage	22-sept-10	22-sept-10	
		L'équipe projet PCRI	nov-10	nov-10	
	1.5 Planning et plans d'actions	Définition, validation du planning et du plan d'action	25-oct-10	25-oct-10	
2 Analyse du contexte et Cartograhie du SI (chap : 4.1.2)	2.1 Inventaire des processus métier	Inventorier l'ensemble des processus fonctionnel du périmètre	sept-10	janv-10	
		Détailler les processus fonctionnels	sept-10	janv-10	
	2.2. Inventaire des actifs	Elements logiciels	oct-10	nov-10	
		Répertorier les actifs matériels, les sites	oct-10	févr-11	
	2.3.Cartographie du SI	Cartographie réseaux et infrastrucure serveur	nov-10	déc-10	
		Cartographier les applications	oct-10	janv-10	
3 Identification des menaces et des risques (chap : 4.1.3)	3.1 Analyse des risques	Analyse méthode SHAM	nov-10	nov-10	
		Analyse des risques GMSIH	sept-10	déc-10	
		Valider les scénarii de risque par le Comité de pilotage	déc-10	déc-10	
		Synthèse des analyses	avr-10	avr-10	
	3.2.Inventaire des besoins en continuité	- Etudier l'ensemble des processus et leurs besoins en continuité	déc-10	déc-10	
		Estimation des durées d'interruption maximales admissibles (et raisonnables)	févr-11	mars-11	
	3.3 conséquenes sur l'activité	- Etudier les impacts potentiels suite aux sinistres	mars-10	mars-10	
		- Valider par la direction	mars-11	mars-11	
4 Synthèse et plan d'action	4.1 Liste de action à mener pour la réduction des risque		oct-10	nov-10	
	4.2 Priorité des traitement de risques		oct-10	nov-10	
	4.3 Définition des solutions de secours	- Définir les solutions de secours en fonction des scenarii de risques et des conséquences	oct-10	nov-10	
	4.4 Plannification et plan d'action		oct-10	nov-10	
5 Elaboration des Plans de continuité	5.1 Procédure de Plan de Crise	Rédaction du Plan de crise	juil-11	oct-11	
	5.2. Procédure Métiers PCM	- Définir l'ensemble des procédures métier pour reprendre l'activité	avr-11	oct-11	
		- Décrire des procédures dégradées pour chaque métier	avr-11	oct-11	
	5.3. Nomination des RPCO	- Nominer un responsable d'un plan de continuité opérationnelle par métier	avr-11	oct-11	
	5.4. Procédures techniques PCRI	- Définir l'ensemble des procédures techniques pour reprendre l'activité	mai-11	nov-11	
		- Décrire des procédures techniques (informatique, courrier)	janv-11	avr-11	
6 Mise en œuvre des sollutions fonctionnelles et techniques de continuité et de reprise	6.1 Déploiement des solutions de secours	Elimier les Spof	oct-10	nov-10	
		- Déploiement et installation des solutions de secours	sept-11	déc-11	
	6.2 Sensibilisation des agents DSI	- Sensibiliser les agents aux procédures de secours techniques et métier	juin-11	août-11	
	6.3 Elaboration des cahiers des charges fournisseu	- Former les agents, les prestataires et les contractants	oct-11	déc-11	
		- Appel d'offres pour acquérier les solutions de secours (site, matériel)	avr-11	nov-12	
	6.4. Mise en place des plans de continuités	- Mobiliser les membres de la cellule de crise	oct-10	nov-10	
		- Mettre en place d'un PCU (Plan de continuité utilisateurs)	oct-10	oct-10	
		- Mise en place d'un PCO (plan de continuité opérationnel)	oct-10	nov-11	
		- Mettre en place un plan de Plan de communication (agents, tiers, partenaires, externes)	oct-10	nov-11	
		- Mise en place d'un PCRI (plan de continuité informatique)	sept-10	nov-11	
7 Déploiement Test MCO (Maintien en Condition Oprérationnel)	7.1. Nomination des CMCO	- Nominer un comité de maintien en condition opérationnelle par métier	oct-11	oct-11	
		- Regrouper les responsables opérationnels dans un comité	oct-10	déc-11	
	7.2. Mise à jour des procédures	- Mettre à jour les procédures suite au déploiement des solutions de secours	oct-10	nov-12	
		- Formaliser les tests	oct-11	nov-12	
		- Valider les temps de reprises exprimés dans les besoins des métiers	nov-11	nov-11	
	7.4 Organisation régulière du PCRI	- Etablir les axes d'amélioration détectées lors des phases précédentes	déc-11	nov-12	
		- Prendre des mesures correctives	déc-11	nov-12	
		- Communiquer ces mesures à l'ensemble des métiers	déc-11	nov-12	
		- S'assurer que les mesures correspondent aux exigences	déc-11	nov-12	

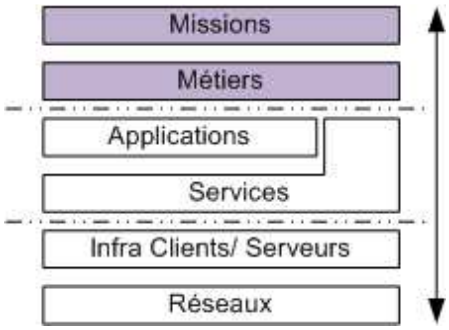
Figure 11 – Extrait planning projet PCRI

4.1.2 ANALYSE DU CONTEXTE ET CARTOGRAPHIE DU SI

L'objectif de ce chapitre est de collecter l'ensemble des éléments nécessaires à l'analyse du projet. Cela passe par une étude de fonctionnement des processus métiers et par l'inventaire des éléments composant le système d'informatique du CHRU de Brest.

4.1.2.1 INVENTAIRE DES PROCESSUS METIER

Dans ce chapitre, je réalise l'inventaire des processus métiers pris en charge par le plan de continuité. Je détaille ces processus et en établis leur enchainement.



Les Missions du CHRU sont le soin, l'enseignement et la recherche.

Etant donné le nombre de processus métiers colossal de l'hôpital et le temps de mon projet de mémoire d'ingénieur, l'ensemble de ceux-ci ne peut être inclus dans le périmètre du plan de continuité. Le plan de continuité ne couvre donc qu'une liste exhaustive de processus métiers. Ces processus métiers ont été sélectionnés et validés par la direction de la DSIS. D'autres processus métiers pourront être inclus dans la démarche PCA ultérieurement.

Les processus métiers compris dans le périmètre du plan de continuité sont les suivants :

- Identification et localisation des patients
- Gestion des laboratoires
- Processus de Soins
- Gestion des dossiers médicaux
- Gestion des services d'urgences

Identification et localisation des patients

2 sous processus

- Identification du patient
- Localisation du patient

L'identification s'effectue par le personnel soignant au travers le logiciel référence (Noyau) dans les services de soins. Au niveau des bureaux des entrées et des accueils d'urgence.

L'ensemble des mouvements patients dans les services de soins est géré par Crossway mouvement. Cette fonction permet d'enregistrer les mouvements des patients au cours de leur hospitalisation (entrée, sortie, passages...) et de préparer la facturation de leur séjour aux tarifs adéquats (lien avec la fonction "facturation").

Dans le cadre des processus de soins et de support, cette fonction permet aussi de "localiser" le patient pour :

- l'acheminement vers l'unité de soins demandeuse des résultats d'examens, des repas et des médicaments.
- l'ouverture des droits d'accès aux éléments de dossier (liens avec les fonctions supportant les processus de soins en plateaux médico-techniques et processus de support). Dans le cadre d'une organisation de santé étendue, cette fonction est susceptible d'évoluer pour prendre en compte les "mouvements" extérieurs à l'établissement.

Liste des services concernés : toutes les unités de soins

Gestion des laboratoires

2 sous processus :

- Gestion des automates
- Mise à disposition des résultats d'analyses

Gestion des automates

Les automates d'analyses sont pilotés par le logiciel Galaxie.

Liste des services concernés : Laboratoires de

- Biologie de la Reproduction
- Génétique moléculaire et Histocompatibilité
- Hématologie
- Immuno-analyse
- Cytogénétique
- Pharmacologie
- Biochimie
- Hygiène hospitalière
- Bactériologie Virologie
- Génétique moléculaire et Histocompatibilité
- Anatomo-pathologie

Mise à disposition des résultats d'analyses

Fonction permettant :

- au niveau des unités de soins et médico-techniques selon autorisation : de consulter les résultats des actes de biologie (lien avec la fonction gestion des comptes-rendus médicaux);
- au niveau des laboratoires : de mettre à disposition les résultats d'analyses (lien avec la fonction supportant le processus de production de soins en laboratoire).

La mise à disposition des résultats d'analyses est effectuée par le bais du logiciel SRI.

Liste des services concernés : toutes les unités de soins

Processus de Soins

Les sous processus de ce processus métier sont :

- Prescription de médicaments
- Prescription Chimio
- Circuit du médicament

Prescription de médicaments

Fonction permettant au niveau des unités de soins : d'aider à la prescription, de formuler la prescription, de la contrôler et de la transmettre à la pharmacie. Au niveau de la pharmacie : de recevoir la prescription, d'effectuer l'analyse pharmaco-économique et de prendre en compte les informations qu'elle contient pour la dispensation (lien avec la fonction supportant le processus de mise à disposition des médicaments).

Le contrôle de la prescription doit être accessible par le prescripteur et le pharmacien et porte notamment sur les contre-indications, les doses et les formes prescrites. La prescription comprend notamment la fréquence et la durée du traitement (lien avec la fonction plan de soins qui permet d'établir le plan d'administration).La prescription concerne les patients hospitalisés (délivrance en ambulatoire).

Prescription Chimio

Fonction permettant de gérer les spécificités inhérentes aux prescriptions de chimiothérapie, notamment la gestion des cycles et cures et la gestion des reconstitutions.

Circuit du médicament

Le circuit du médicament est composé d'une série d'étapes successives, réalisée par des professionnels différents : la prescription est un acte médical, la dispensation, un acte pharmaceutique et l'administration, un acte infirmier ou médical. En outre, ce circuit est interfacé avec le système d'information hospitalier et la logistique. Chaque étape de ce circuit est source d'erreurs potentielles qui peuvent engendrer des risques pour la santé du patient.

Service concerné : cardiologie 2

Gestion des dossiers médicaux

Fonction permettant l'organisation du travail infirmier comprenant :

- le plan de prélèvement et la constitution du compte-rendu de prélèvement ;
- le plan d'administration des médicaments et la constitution du compte-rendu d'administration et du compte-rendu de suivi thérapeutique
- le plan de soins paramédicaux.

Fonction permettant l'enregistrement des observations et des transmissions infirmières, standard ou ciblées, ainsi que les informations relatives à la charge en soins.

Services concernés : toutes les unités de soins

Gestion des services d'urgences

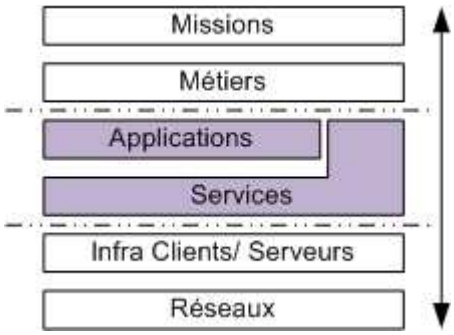
L'accueil et le traitement des urgences est une des fonctions première du CHRU. Cela concerne l'accueil des malades et des blessés se présentant spontanément ou amenés par des ambulances ou véhicules de prompt-secours des sapeurs-pompiers. Le rôle d'un service d'urgences est d'accueillir sans sélection vingt-quatre heures sur vingt-quatre, tous les jours de l'année, toute personne se présentant en situation d'urgence, y compris psychiatrique, et de la prendre en charge, notamment en cas de détresse et d'urgence vitales.

Liste des services concernés :

- Accueil Urgence de la Cavale Blanche et de Carhaix
- Accueil Urgence Pédiatrique de Morvan
- CE Accueil Urgence Vitale
- CE Urgence Psychiatriques
- CE Urgence Chirurgicales
- CE Urgence Médicales
- Urgence Gynécologiques de Morvan et de Carhaix

4.1.2.2 INVENTAIRE DES ACTIFS

Cartographie Logiciel



Une classification spécifique des logiciels est mise en œuvre et sera complétée au fur et à mesure du projet et des études associées. Pour compléter ce catalogue, je me suis fait aider par Isabelle Cortes Ingénieur Process de la DSIS. Les mises à jour de ce fichier sont validées par le comité de pilotage régulièrement.

Microsoft Excel - Catalogue_ des_applications.xls

Fichier Edition Affichage Insertion Format Outils Données Fenêtre ?

P2 Fonctions SI

	B	I	J	K	L	M	N	O
1								
2	Services/ Fonction	Services/ Fonction	Services/ Fonction	Services/ Fonction	Services/ Fonction	Services/ Fonction	Services/ Fonction	Services/ Fonction
48	Gestion des appels d'offres	EPICURE	Pharmacie & S. économiques	R. CLOAREC	A. MINGAM	Mme BECHU	PHARMATIC	Administratif
49	Gestion des Applications Web	GDA	DSIS	D. SEBASTIA	F. LE BEC		AXETIC (pas de contrat)	Technique
50	Gestion des certificats pour la gestion des marchés	OMNICLES	Administratifs	P. MENOU	A. ROBBE			Technique
51	Gestion des demandes d'interventions utilisateurs	INTERVENTIONS	DSIS	R. Le BARS			DSIS / Fllemaker	Technique
52	Gestion des demandes de linge banalisé	GESTLINGE	CTT Unités de soins	D. SEBASTIA	F. LE BEC	Mr MOREAU (CTT) Mme STEPHAN (CTT)	Logiciel libre	Médico-administratif
53	Gestion des déports consoles via IP	Console KVM IP	DSIS	P. MENOU	A. ROBBE			Technique
54	Gestion des dossiers médicaux	MO ARCHIVES	Secrétariats médicaux et archives	G. BILHANT	F. CAM	R. REBOUR	MEDIWARE	Médico-administratif
55	Gestion des éléments réseaux	ELEMENTS RESEAUX	DSIS	P. MAYANCE	E. GUIZIOU		DSIS	Technique
	Gestion des greffes &							

Figure 12 – extrait du catalogue des applicatifs CHRU

Au fil des années le nombre de logiciel SI n'a cessé de croitre. Les interconnexions et interdépendances font que le SI est de plus en plus complexe.

Lors de l'intégration de l'hôpital de Carhaix en 2009 au CHRU de Brest, la cartographie ci-après a été réalisée par Jean Pierre Pallier, responsable Groupe Applications Métiers à la DSIS. Celle-ci est toujours à jour en ce qui concerne les logiciels inclus dans le périmètre de l'étude PCRI.

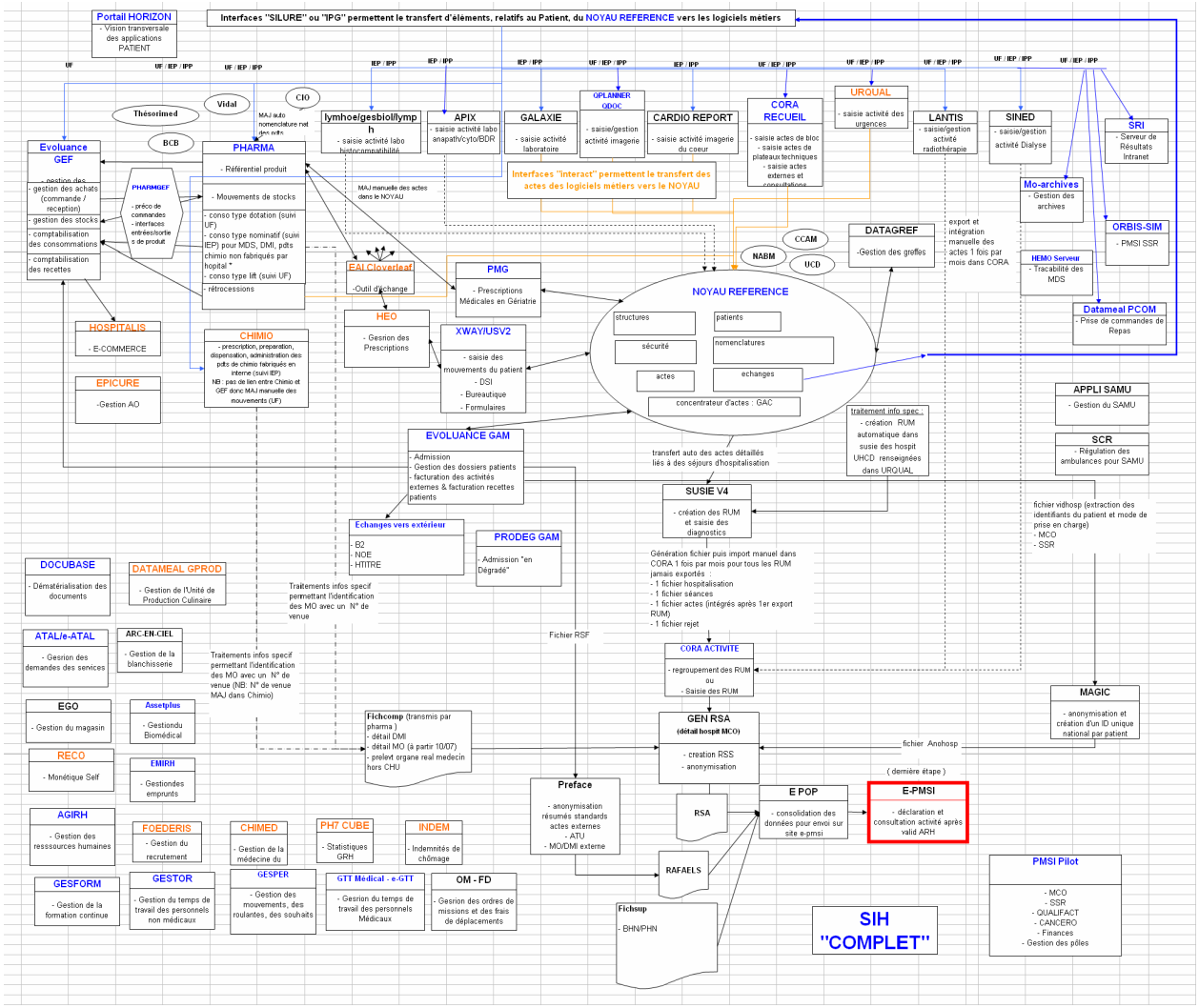
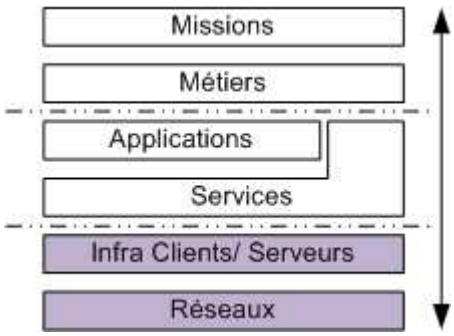


Figure 13 – extrait de la cartographie des applicatifs CHRU

Cartographie infrastructures et réseaux

Architecture réseaux



Le Centre Hospitalier Régional Universitaire de Brest est composé de sept établissements principaux:

L'hôpital Morvan situé au centre ville de Brest héberge les salles serveurs principales. Le service Informatique du CHRU y est implanté, cet établissement est le cœur du SIH.

L'hôpital de la Cavale Blanche, situé à la périphérie de Brest, est distant de 5 Km du site de Morvan. Le site est relié au site de Morvan par des liaisons fibres monomodes, d'un débit de 2Gb/s vers chaque cœur de réseau. Un lien de secours s'effectue via le réseau Métropolitain (MAN) de la ville de BREST avec un débit de 1Gb/s.

L'hôpital de Bohars, situé dans l'agglomération Brestoise, est distant de 5 Km de l'hôpital Morvan. Le lien principal s'effectue via le réseau Métropolitain (MAN) de la ville de BREST avec un débit de 1Gb/s.

Une liaison HYPERLAN 2, d'un débit de 10Mbits/s, assure le secours.

Le Centre René Fortin, situé dans l'agglomération brestoise, est distant de 5 Km de l'hôpital Morvan. Il jouxte l'hôpital de Bohars. Le site est relié au site de MORVAN via une liaison SDSL 4 Mb/s. Une liaison HYPERLAN 2, d'un débit de 4 Mb/s assurera le secours.

L'hôpital Ponchelet, situé dans la ville de Brest, est distant de 2,5 Km du site de Morvan. Le site est relié au site de MORVAN via une liaison SDSL 4 Mb/s. Une liaison HYPERLAN 2, d'un débit de 4 Mb/s assurera le secours.

L'hôpital de Guilers, situé à la périphérie de Brest, est distant de 6 Km du site de Morvan. Le lien principal s'effectue via le réseau Métropolitain (MAN) de la ville de BREST avec un débit de 1Gb/s. Une liaison ADSL assure le secours.

L'hôpital de Carhaix, distant d'environ 80 Km du site de Morvan. Le nouveau raccordement vers le réseau BIPS est composé d'une liaison fibre optique 10Mb/s avec un secours passif par une liaison SDSL 4Mb/s. Ces liaisons sont opérées par l'opérateur du réseau BIPS (SFR)

Le Centre Hospitalier Régional Universitaire de Brest a fait le choix de la technologie Ethernet (10/100/1000) en 2001. En 2004, pour renforcer la sécurité de son réseau, le CHRU de BREST a fait le choix d'une architecture de niveau 3 (routage) et du protocole OSPF. IP est le protocole fédérateur du réseau. La définition actuelle des adresses IP des serveurs s'effectue de manière statique et de manière dynamique pour les stations et imprimantes.

Les serveurs DNS Internes et DHCP sont installés sur des serveurs Windows Server 2003. Le réseau IP du CHRU est constitué de plusieurs VLANS, correspondant chacun à un plan d'adressage spécifique, permettant de regrouper, au maximum, 500 machines. L'épine dorsale est composée de 4 Commutateurs Enterasys Matrix E7-N7, reliés entre eux par des liaisons 2 X Gigabit Ethernet et utilisant le protocole OSPF pour communiquer.

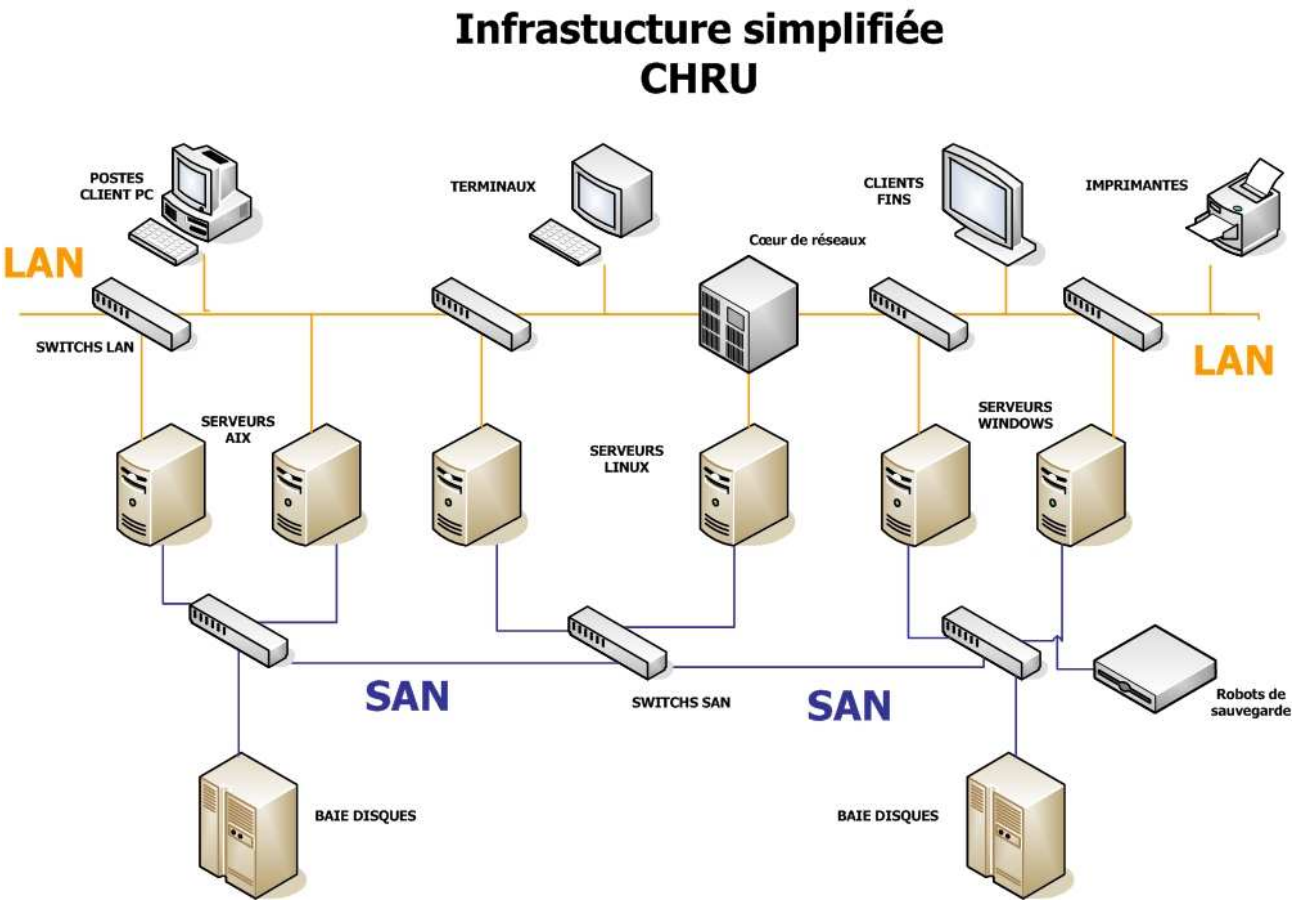


Figure 14 – schéma simplifié de l'infrastructure SI du CHRU

Architecture SAN

Le CHRU dispose d'un SAN composé de 2 baies de disques HP (EVA8100) totalisant environ 30 To. Les données sont répliquées entre les baies.

Les sauvegardes sont assurées par une VTL QUANTUM DX5000 de 9To et un robot QUANTUM Scalar I500, 2 lecteurs LTO4, 82 alvéoles, 64To. Le logiciel de sauvegarde centralisée est HP DATA PROTECTOR

Architecture Serveurs

Serveurs AIX :

10 serveurs de type AIX en version 5 dont 8 en géo cluster (2 racks et 8 lames)

Serveurs Linux (Red Hat ES 4 ou ES5) :

2 serveurs de type rack et 12 serveurs lames type x86

Serveurs Microsoft :

10 serveurs Windows 2000 ou 2003 format rack,

27 serveurs Windows 2003 de type « lame » répartis dans 2 châssis HP et 2 châssis BULL

26 serveurs virtuels (Virtual Server 2005 R2), boot SAN

Postes Clients

Postes de travail de type PC/PC portable : environ 2900 postes

Terminaux Clients Légers : environ 200

Terminaux Clients Légers Portables : 120

Imprimantes : environ 500

4.1.2.3 RECENSEMENT

J'ai entrepris une classification de l'ensemble des actifs Informatiques. Le but est de recenser l'ensemble des biens liés au processus informatique et d'y indiquer les mesures de sécurité associées. On y trouvera les éléments tels que les locaux informatiques, les éléments réseaux, les serveurs, les éléments SAN ….. Ce document est mis à jour par les groupes concernés.

	A	B	C	D	E	F	G
				Mesures de sécurité			
	Zone	Site	Localisation	Accès	Incendie	Risques innondations	Climatisation
	Salle machine	Morvan	Bat 5 Bis NIV -1	- 2 niveaux d accès (DSIS & SM) - lecteur de carte sans contact & digicode - fenêtre protégée par grille - traçabilité des accès - détecteur de mouvement dans le couloir	- Détecteur incendie (type : ionisation, optique, flamme, thermique) - protection au ??? - déclencheur d'alarme ? - porte coupe feu?	Détecteur ???	Climatisée
	Salle machine BIS	Morvan	BAT 1 NIV 3				
	Salle sauvegarde	Morvan		- salle "noire" - digicode + clé - Pas de traçabilité des accès - Pas d'alarme	- Détecteur incendie		
	Salle stockage des bandes	Morvan					
	Salle SAMU 29	Cavale Blanche		- Accès par la permanence du SAMU. Digicode de l'intérieur mais accès possible de l'extérieur			
1	SRI01	Cavale Blanche	Pharmacie				
2	SRI02	Cavale Blanche	Service technique niv. -2				
3	SRI03	Cavale Blanche	Urgence niv. -1				

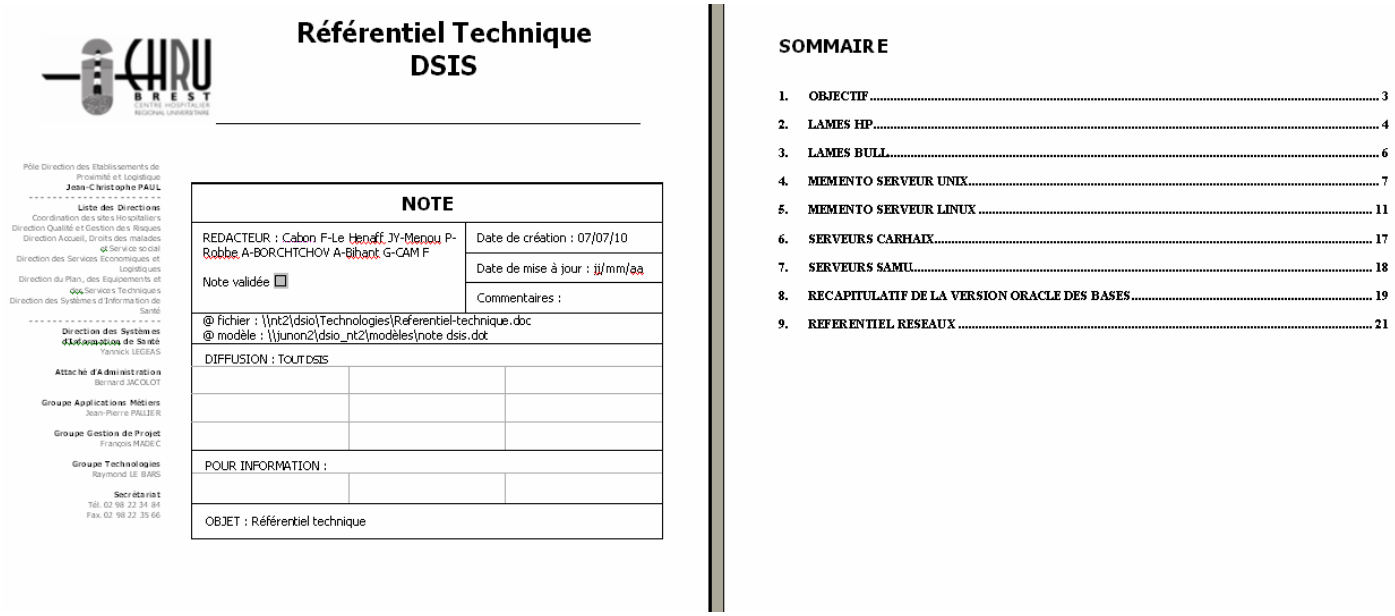
Locaux | Point d'accès Internet | Elements réseaux | Elément Wifi | Elements de sécurité | Serveurs | Sauvegardes | San | Services infrastruct

Figure 15 – extrait des actifs SI CHRU

Il existe plusieurs documents référençant les éléments techniques. Chaque binôme (ref organigramme DSIS) crée et met à jour ses propres documents techniques. La conséquence de cette façon de faire est une redondance des informations dans plusieurs documents et une dispersion des informations : les informations se situent dans différents répertoires partagés et parfois sur des serveurs différents.

J'ai mis à disposition des équipes du groupe technologies un document unique. Celui-ci devient le référentiel unique. Chaque mise à jour y est notifiée et datée. Dorénavant, chaque nouvelle information et nouveau document technique doivent y être reportés.

Ce référentiel technique sera bien évidement un élément principal du plan de continuité. A la survenance d'une panne majeure, ce fichier sera d'une grande utilité.



Référentiel Technique
DSIS

Pôle Direction des Etablissements de Proximité et Logistique
Jean-Christophe PAUL

Liste des Directions
Coordination des sites Hospitaliers
Direction Qualité et Gestion des Risques
Direction Accueil, Droits des malades et Service social
Direction des Services Economiques et Logistiques
Direction du Plan, des Equipements et des Services Techniques
Direction des Systèmes d'Information de Santé

Direction des Systèmes d'Information de Santé
Yannick LEDEAS

Attaché d'Administration
Bernard JACOLOT

Groupe Applications Métiers
Jean-Pierre PALLIER

Groupe Gestion de Projet
François MADEC

Groupe Technologies
Raymond LE BARS

Secrétariat
Tél. 02 98 22 34 84
Fax. 02 98 22 35 66

NOTE	
REDACTEUR : Cabon F-Le Henaff JY-Menou P-Robbe A-BORCHTCHOV A-Bihant G-CAM F Note validée ☐	Date de création : 07/07/10 Date de mise à jour : jj/mm/aa Commentaires :
@ fichier : \\nt2\dsio\Technologies\Referentiel-technique.doc @ modèle : \\junon2\dsio_nt2\modèles\note dsis.dot	
DIFFUSION : TOUT DSIS	
POUR INFORMATION :	
OBJET : Référentiel technique	

SOMMAIRE

Figure 16 – Extrait du référentiel technique

4.1.3 IDENTIFICATION DES MENACES ET DES RISQUES

4.1.3.1 ANALYSE DES RISQUES

Le but est de mener une analyse des risques et donc de la sécurité du SI dans sa globalité. Il faut identifier les menaces potentielles et leurs probabilités d'occurrence. Cette étude doit déterminer une liste exhaustive de scénarii de pannes, auquel je devrais proposer des contre-mesures et piloter leur mise en œuvre.

L'analyse a été menée en 2 étapes. Une première étape est réalisée via la méthode SHAM. Cette méthode m'a été présentée par l'ingénieur gestion des risques monsieur Jean François Calvar. Je l'ai adaptée à la problématique informatique et l'ai associée aux menaces référencées dans la méthode EBIOS. La méthode SHAM est mise à disposition par l'assureur des établissements de santé.

Pour la deuxième étape de mon étude, j'ai appliqué la méthode publiée par le GMSIH à savoir le GAE (Guide d'auto évaluation). Cette méthode reprend les grandes lignes de la norme iso27002, mais est spécialement élaborée pour être appliquée aux SIH (Système d'Information Hospitalier). Sa mise en œuvre et son analyse se sont effectués avec la participation de monsieur Stéphane Gouarnison du GCS (Groupe de Coopération Sanitaire) responsable du comité projet démarche SSI régionale.

Une analyse de risques plus poussée et au périmètre élargie sera réalisée par une société spécialisée courant 2012. Cette prestation est inscrite dans le lot 2 du CCTP SSI d'UNI-HA auquel le CHRU a adhéré.

Analyse méthode SHAM

L'objectif de cette étape est de cartographier les sinistres contre lesquels l'hôpital cherche à se prémunir. Pour ce faire, dans un premier temps j'ai dressé un panorama des menaces qui pèsent sur l'établissement de santé.

Listes des menaces référencées dans la méthode EBIOS.

	Sinistre physique
1	- Dégâts des eaux (fuite, rupture de canalisation, déclenchement des systèmes d'extinction, vandalisme,...)
2	- Explosion,
3	- Incendie (foudre, court-circuit,...)
4	- Sinistre majeur
	Evénements naturels
5	- Phénomène climatique (froid, humidité, chaleur, vent, sécheresse,...)
6	- Phénomène sismique
7	- Phénomène météorologique (tempête, inondation, grêle, foudre,...)
	Perte de Services essentiels
8	- Défaillance de la climatisation
9	- Perte d'alimentation énergétique
10	- Perte des moyens de télécommunication
	Compromission des informations
11	- Attaque logique ciblée (destruction manuelle d'information, denis de service,...)
12	- Infection par un virus, un ver, ...
13	- Information sans garantie de l'origine
14	- Récupération de supports recyclés ou mis au rebus
15	- Sabotage d'un matériel
16	- Vol de matériel (informatique, télécom, bio-médical,...)
17	- Vol de support, de données, d'information
	Défaillance technique
18	- Atteinte à la maintenabilité du SI
19	- Dysfonctionnement logiciel
20	- Dysfonctionnement matériel
21	- Panne matérielle
22	- Saturation du système informatique
	Actions illicites
23	- Altération des données
24	- Copie frauduleuse de logiciels
25	- Divulgation de données personnelles, médicales, confidentielles
26	- Indiscrétion dans un ordinateur pendant une absence
27	- Intrusion ou tentative d'intrusion de système d'information
28	- Non respect de la politique de sécurité
29	- Traitement illicite des données
30	- Utilisation de logiciels contrefaits ou copiés
31	- Utilisation illicite des matériels
	Compromission des fonctions
32	- Abus de droit
33	- Acte de chantage ou d'extorsion informatique
34	- Acte de dénigrement ou d'atteinte à l'image,
35	- Atteinte à la disponibilité du personnel
36	- Erreur d'utilisation
37	- Fraude informatique ou télécom (détournement de fond, ...)
38	- Reniement d'actions
39	- Usurpation de droits

Figures 17 – Inventaires des menaces selon Ebios

Cartographie des risques

Le but de cette cartographie est d'évaluer pour chaque menace la probabilité d'occurrence et l'impact potentiel de la menace sur les processus jugés critiques.

Pour ce faire les risques sont catégorisés et regroupés en scénarii selon leur type et leur impact potentiel. L'évaluation du risque se fera selon 2 critères : L'impact (potentiel du risque) et la probabilité que le risque survienne. Au terme de cette étape, une cartographie des sinistres ainsi que les scénarii de sinistres retenus doivent être livrés.

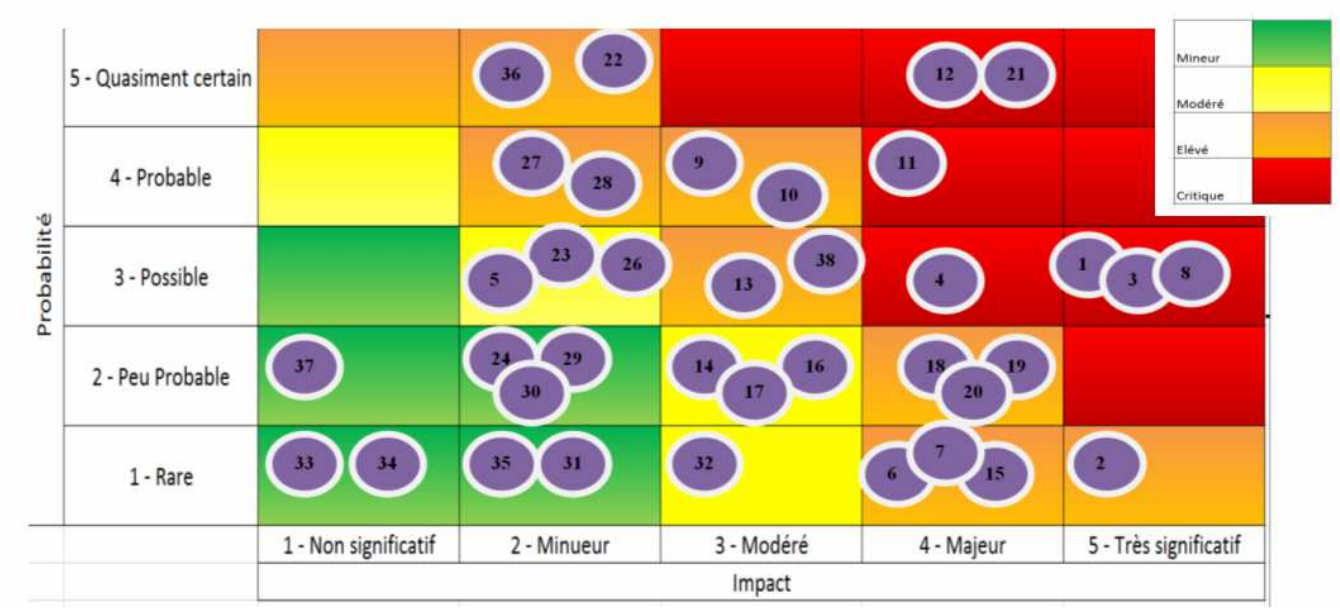


Figure 18 - Cartographie des risques

Impact	
1 - Non significatif	Evènement dont l'impact peu être absorbé par l'activité normale
2 - Mineur	Evènement dont l'impact peu être absorbé mais nécessitant une intervention pour en minimiser l'impact
3 - Modéré	Evènement majeur pouvant être géré dans des circonstances normales
4 - Majeur	Evènement critique supportable moyennant une gestion de crise correcte
5 - Très significatif	Désastre susceptible de provoquer l'effondrement de l'entreprise

probabilité	Pourcentage	
1 - Rare	< 10 %	Evènement risquant de se produire uniquement dans un cas exceptionnels
2 - Peu Probable	10-30 %	Evènement risquant de se produire à un moment donné
3 - Possible	30-50 %	Evènement devant se produire à un moment donné
4 - Probable	50-90 %	Evènement probable dans la plupart des cas
5 - Quasiment certain	> 90 %	Evènement attendu dans la plupart de cas

Liste des menaces à prendre en compte suite à l'analyse des risques SHAM :

Sinistres physiques affectant un bâtiment (locaux) : incendie, inondation

Défaillances techniques

Indisponibilité du personnel informatique : pandémie

Défaillances fournisseurs de services : EDF

Attaques virales (Infection par un virus, un ver …)

Analyse des risques GMSIH

L'analyse des risques GMSIH s'effectue par l'outil GAE. Cet outil s'utilise au travers d'un formulaire.

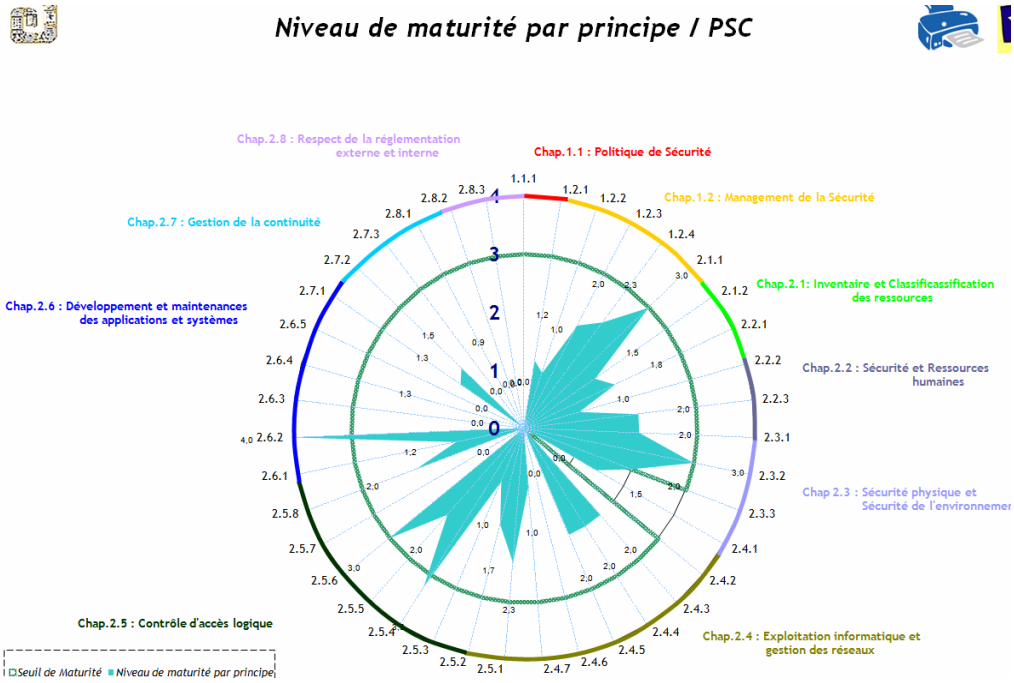


Figure 19 – niveau de maturité extrait de l'outil d'analyse de risque GAE

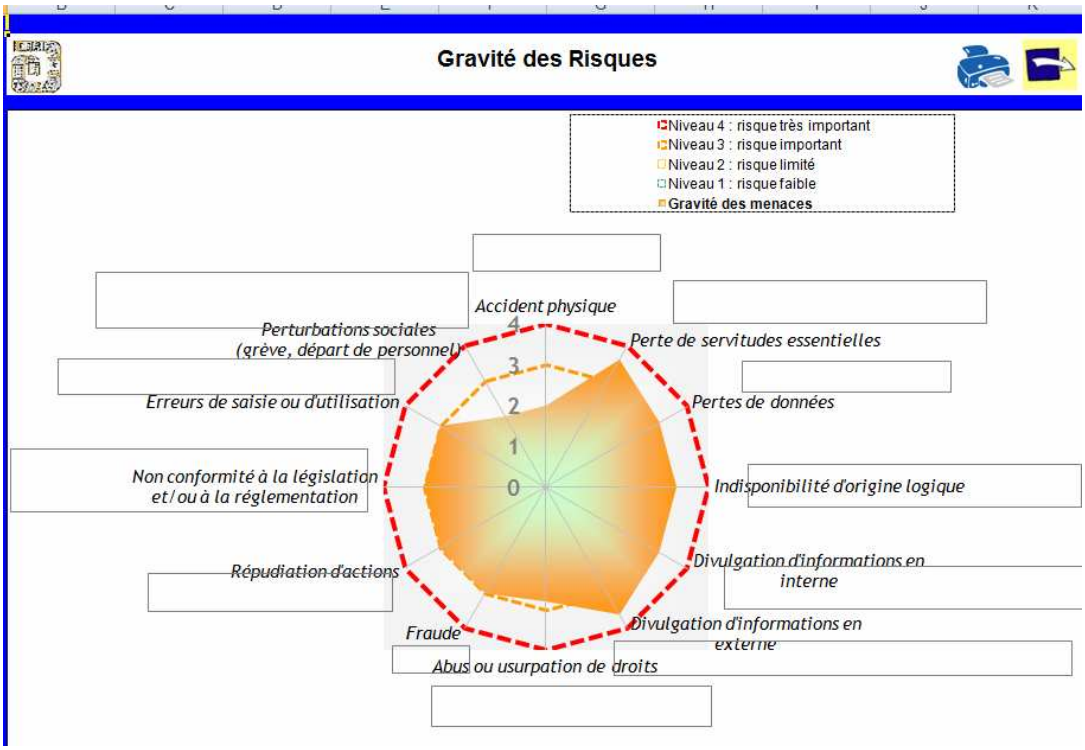


Figure 20 – gravité des risques, extrait de l'outil d'analyse de risque GAE

Efficacité des principes en réduction des risques

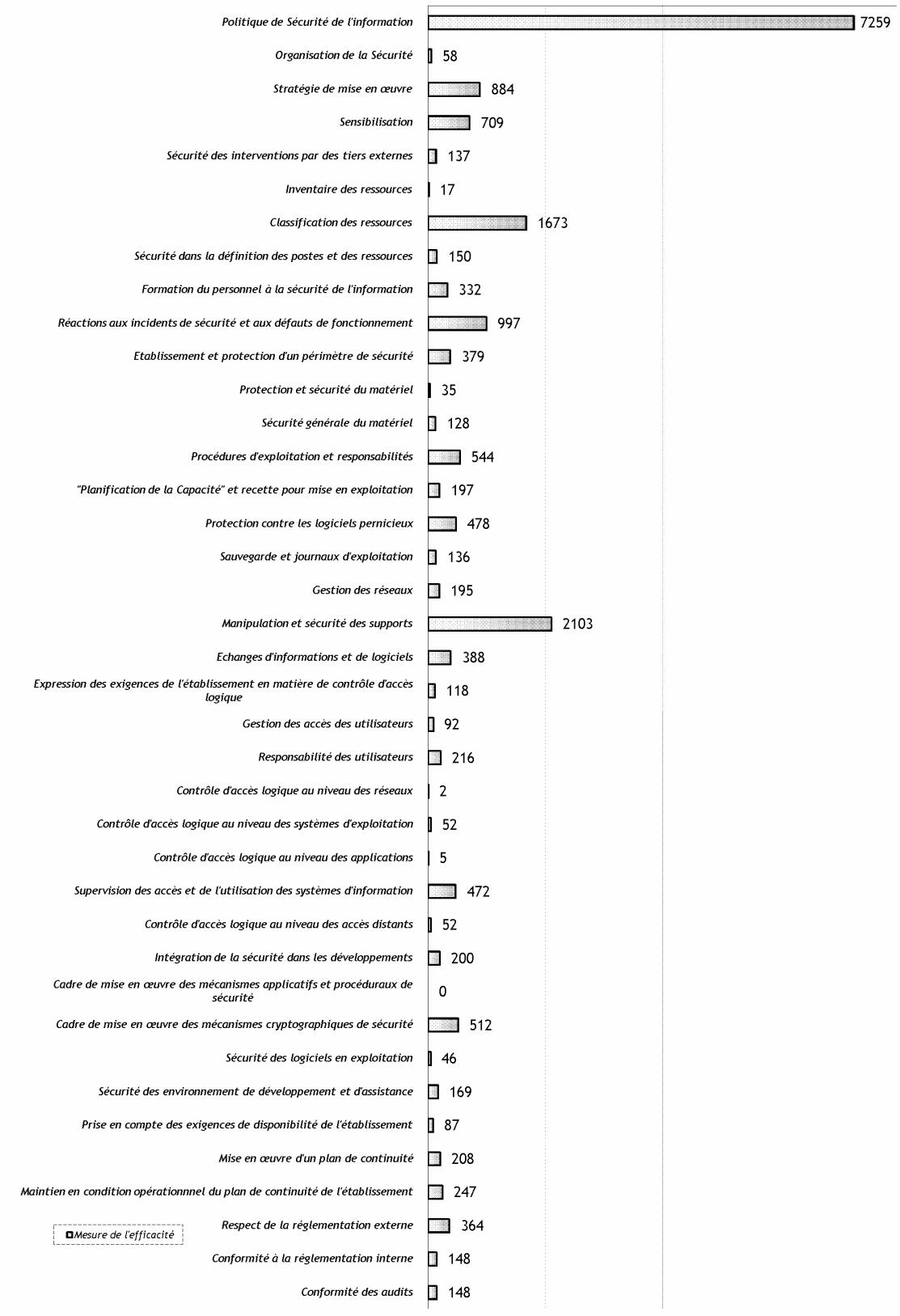


Figure 21 – Synthèse de l'analyse de risque GAE

4.1.3.2 SYNTHESE DES ANALYSES

Liste des menaces à prendre en compte suite à l'analyse des risques SHAM :

- Sinistres physiques affectant un bâtiment (locaux) : incendie, inondation
- Défaillance techniques
- Indisponibilité du personnel informatique : pandémie
- Défaillance fournisseurs de services : EDF
- Attaques virale

De ces menaces les scénarii de sinistres suivants ont été retenus :

- Perte d'un cœur de réseaux incident électrique
- Perte d'une des baies SAN par incident électrique
- Perte d'un des châssis lames incident électrique
- Perte totale d'une des salles informatiques par incendie ou inondation
- Infection virale de plus de 100 postes clients
- Défaillances fournisseurs de services : EDF, SFR
- Indisponibilité du personnel informatique : pandémie

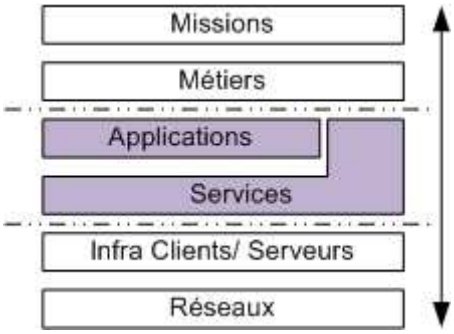
Cette liste de scénarii a été proposée et validée par l'équipe de pilotage.

4.1.3.3 INVENTAIRE DES BESOINS EN CONTINUITE

Dans ce chapitre, j'étudie l'ensemble des processus et leurs besoins en continuité. Pour ce faire, je dresse dans un premier temps la liste exhaustive des logiciels utilisés et nécessaires à la réalisation des processus métiers. Dans un second temps, je fais estimer les durées d'interruption maximales admissibles pour chaque logiciel. L'objectif étant de déterminer le plus précisément le besoin de continuité de chaque logiciel par rapport aux processus métiers.

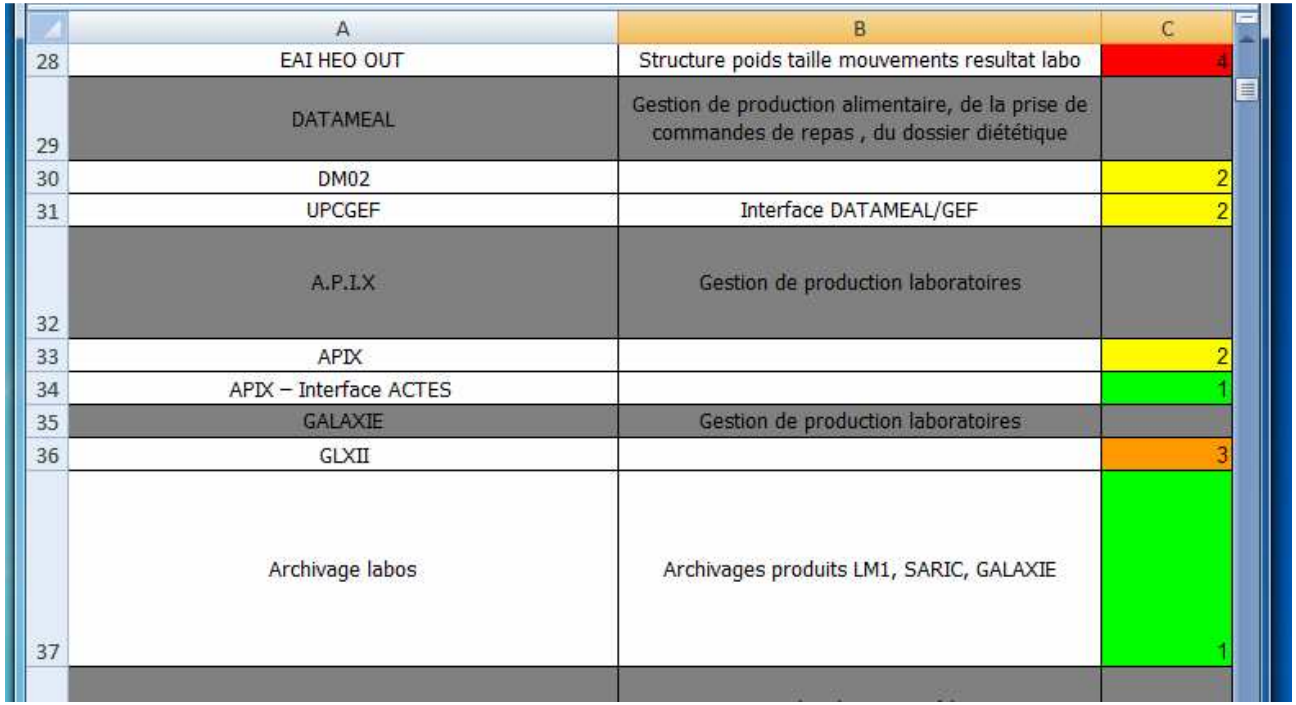
Les processus métiers compris dans le périmètre du plan de continuité sont les suivants :

- Identification et localisation des patients
- Gestion des laboratoires
- Processus de Soins
- Gestion des dossiers médicaux
- Gestion des services d'urgences



Afin de déterminer au mieux le Bilan de l'Impact sur les Activités (BIA) du périmètre projet, il est essentiel de juger au mieux de la criticité des logiciels métiers. Un logiciel métier peut se composer d'applications, de bases de données ou d'interfaces. Une interface étant un programme permettant l'interconnexion entre logiciels ou bases de données. Pour ce faire j'ai défini pour l'ensemble des logiciels compris dans le projet, le Délai d'Interruption Maximale Admissible (DIMA). Bien entendu la définition du DIMA s'est faite par des personnes ayant une grande connaissance des fonctions des logiciels et une expérience certaine des métiers et de leurs missions. Le tableau suivant a donc été complété par Jean Pierre Pallier responsable application DSIS et François Madec responsable projet DSIS.

Délai d'Interruption Maximale Admissible par logiciels métiers



	A	B	C
28	EAI HEO OUT	Structure poids taille mouvements resultat labo	4
29	DATAMEAL	Gestion de production alimentaire, de la prise de commandes de repas , du dossier diététique	
30	DM02		2
31	UPCGEF	Interface DATAMEAL/GEF	2
32	A.P.I.X	Gestion de production laboratoires	
33	APIX		2
34	APIX – Interface ACTES		1
35	GALAXIE	Gestion de production laboratoires	
36	GLXII		3
37	Archivage labos	Archivages produits LM1, SARIC, GALAXIE	1

Figure 22 – Extrait du référentiel regroupant la liste exhaustive des applications métiers

Niveau	Disponibilité
4	**Interruption <= 15 min**
	Les informations doivent être accessibles en permanence et utilisables par tous les services concernés
3	**Interruption <= 1 h**
	Les informations doivent toujours être fournies pour remplir le service attendu.
2	**Interruption <= 8 h**
	Une indisponibilité momentanée est tolérée, mais doit être signalée et sans conséquence sur le service fournit
1	**Interruption <= 3j**
	Une indisponibilité temporaire est acceptable.

4.1.3.4 CONSEQUENCE SUR L'ACTIVITE

Afin de visualiser d'une manière rapide et claire l'impact de l'arrêt de telle ou telle application, interface ou encore base de donnée, j'ai mis au point un nouvel outil. Avec l'ensemble des éléments et documents recueillis, j'ai initialisé une nouvelle cartographie regroupant les éléments compris dans le périmètre du plan de continuité. Pour la mise en œuvre j'ai privilégié le logiciel de cartographie Microsoft Visio car déjà utilisé à la DSIS. Le fichier Excel de référence « référentiel-Caro.xls » est directement lié au logiciel Visio, ainsi toutes les informations comprises sur la cartographie sont simplement mises à jour. Le nouveau référentiel est mis à jour par mes soins, celui-ci regroupe les informations contenues dans le référentiel technique et le catalogue des applications.

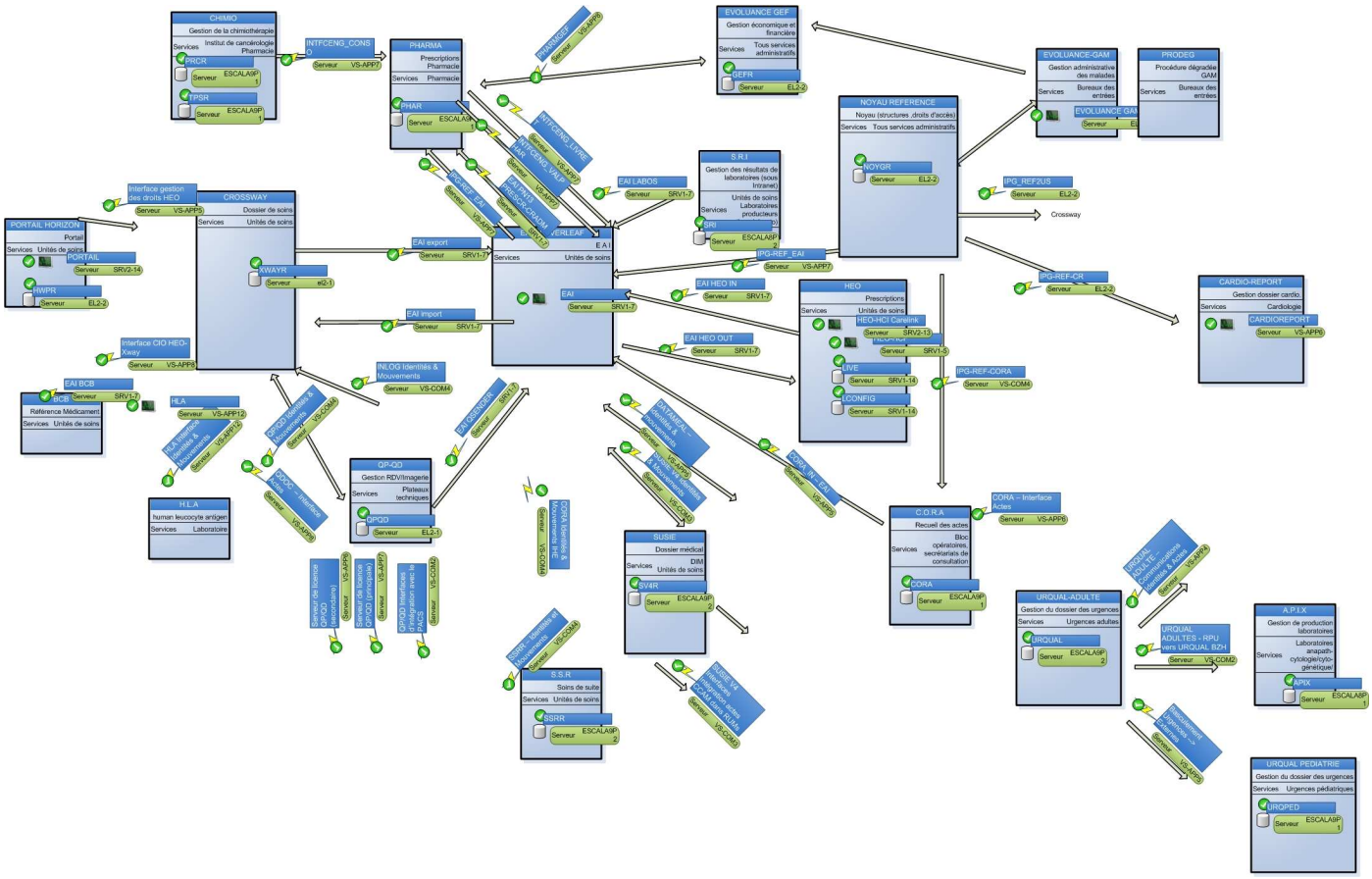
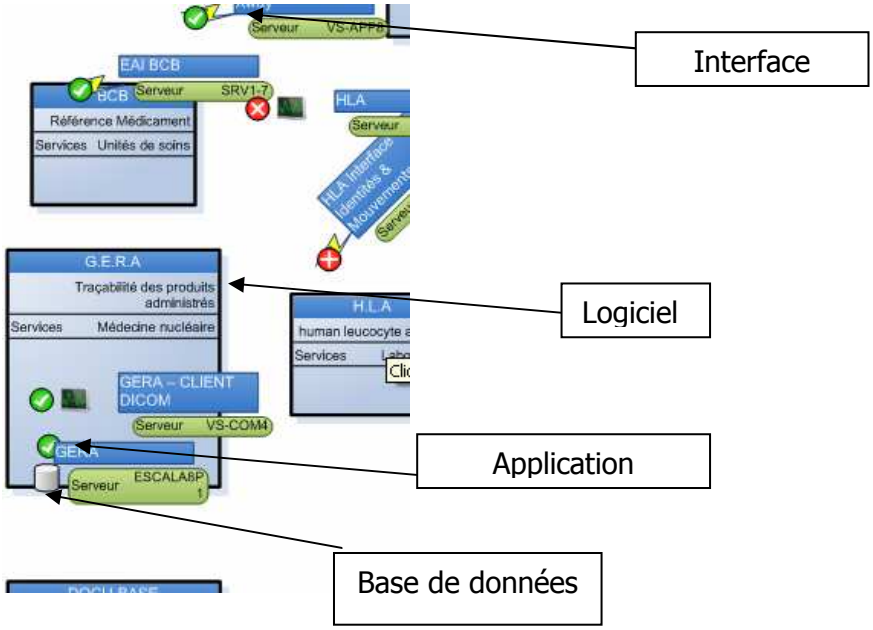


Figure 23 – Extrait de la cartographie d'impacts applicatifs

Signification des symboles et légendes



Il s'agit de la représentation d'une partie des logiciels (périmètre PCRI) et de leurs interactions dans le SI.

En plus d'une cartographie du SI, cet outil permet de réaliser un bilan d'impact rapide, c'est-à-dire de simuler l'impact sur le SI de la perte de tel ou tel élément système.

4.1.3.5 CONSEQUENCES DES SINISTRES-INCIDENTS RETENUS

Cette analyse de conséquence de sinistres est essentielle à la rédaction des plans de continuité et de reprise.

Rappels des scénarii des sinistres-incidents retenus :

A - Perte d'un cœur de réseaux incident électrique

B - Perte d'une des baies SAN par incident électrique

C - Perte d'un des châssis lames incident électrique

D - Perte totale d'une des salles informatiques par incendie ou inondation

E - Infection virale de plus de 100 postes clients

F - Défaillances fournisseurs de services : EDF, SFR

G - Indisponibilité du personnel informatique : pandémie

A - Perte d'un cœur de réseaux incident électrique

Le CHRU a fait le choix d'une architecture de niveau 3 (routage) et du protocole OSPF (Open Shortest Path First). Ce protocole permet de couvrir actuellement un nombre de pannes important liées à la perte d'un élément réseau. Malheureusement, l'architecture réseau actuelle des sites du CHRU ne permet pas une couverture complète par ce protocole. En effet, les réseaux fibres les plus anciens sont composés d'un seul lien. De plus le coût est un sérieux frein au déploiement de doubles liens fibres. De ces deux dernières problématiques, j'ai mené une étude permettant de définir les conséquences sur les services lors de la survenance d'une panne sur un élément actif réseau. Le but est de classer les services par criticité et ainsi définir quels sont les services les plus critiques à prioriser et à couvrir par l'OSPF.

Pour ce faire, j'ai réalisé un regroupement de la base de données parc et l'outil de supervision réseau What's Up.

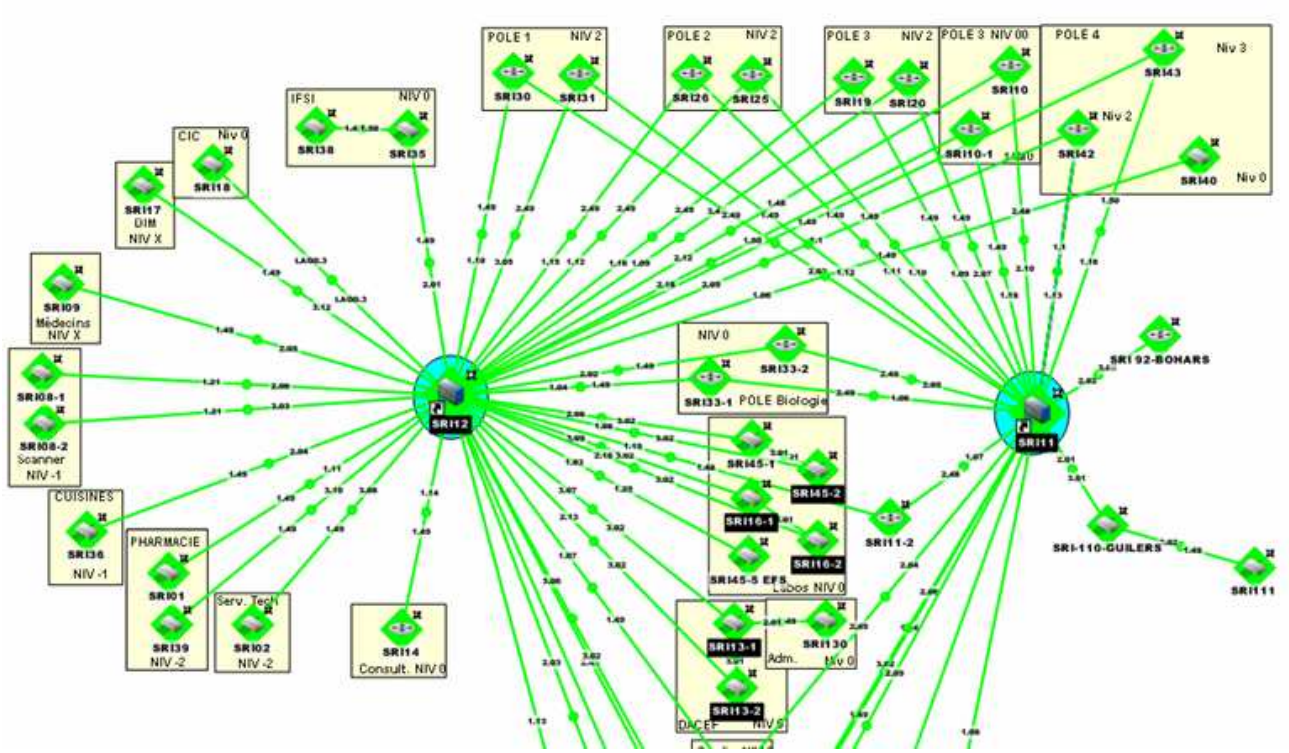


Figure 24 – Extrait du logiciel What's Up

	A	B	C	D	E
1	SRI	Pole / Batiment	Niveau	Services	Criticité Services
2	Cavales Blanches Conséquences Pertes SRI 12				
3	12	P.T.	X	Bureaux Médecins Niv X	3
4	35	ParaMédical	0	Ecoles de Formation IBODE / IADE	2
5	38	PARAMEDICAL	0	IFSI Ecoles INFIRMIERES	2
6	18	P.T.	0	Med. Interne 1 et PneumoCIC	2
7	17	P.T.	0	D.I.M. Archives	2
8	9	P.T.	X	Bureaux de Médecins Niv X	3
9	8	PT	-1	IMAGERIE MEDICALE	4
10	36	Cuisines	-1	Cuisine Centrale Magasins	2
11	1	P.T.	-2	CAMSP Pharmacie CB	2
12	39	CAMSP	-2	Pharmacie	2
13	2	P.T.	-2	Services Techniques CB Caisson HyperBare Urgences Médicales (Médecin) Urgences Psychiatriques (Médecin)	2
14	14	P.T.	0	Chirurgie Viscérale Endocrinienne (Cons.) Explorations Fonctionnelles Neurologiques Médecine Interne 2 Maladies Infectieuses Orthopédie / Traumatologie Neurologie Neurochirurgie (Consult.) Rhumatologie	2
15	45	P.T.	0	E.F.S. Labo. Anapathologie Labo. Chimie A Labo. Pharmacologie	4
16	16	P.T.	0	Labo. Hématologie Labo. Pharmacologie	4
17	130	P.T.	0	Bureau des Entrées Direction Services Economiques Direction C.B. D.S.S.I. Direction Ressources Humaines Medecine Préventive Service Social	2
18	40	4	0	Anesthésie-Réanimation Hépato-Gastro-Entérologie	4
19	Morvan Conséquences Pertes SRI 68				
20	68	5 BIS	S/Sol	NIV -1: Salle Informatique Niv -1 : IRM BAT 5 Bis NIV 0 : Planning Familial	2
21	72	FAC	2	Labo Cytogénétique	2
22	62	4	6	Ophtalmologie Dermatologie Explorations Fonctionnelles Neurologiques ORL	2
23	77	7	0	Labo. Anapath Standard	2
24	76	7-BCE	RdC	Pharmacie Morvan Services Economiques (Cartes Repas) Bureau des Entrées (Contentieux) SELF Labo HLA	2
25	66	5	7	NIV 2 : Gynécologie NIV 3 : Réanimation Ped, Néonat NIV 4 : Pediatrie G.E., Génétique, Pédiatrie NIV 5 : Pédiatrie Nourrissons NIV 6: Chirurgie Pédiatrique	2

Figure 25 – Extrait fichier criticité services

B - Perte d'une des baies SAN par incident électrique

Le cas de la perte « partielle » d'une des baies est déjà apparu le 16 juin ; Il s'agissait d'une perte d'un des contrôleurs.

Intervention Informatique le Mercredi 16 Juin 2010

Bonjour,

La détection d'une anomalie technique sur l'infrastructure "disques" d'une des salles informatiques nous a contraint à programmer **une intervention en URGENCE pour travailler à la résolution du problème.**

Cette intervention est planifiée le 16/06/2010 à partir de 17H.

En fonction du résultat des premières opérations techniques, il est possible que nous soyons contraints d'arrêter certains logiciels. Ces interruptions seront de courte durée (entre 1/4 d'heure et 1/2 heure) pour les logiciels qui bénéficient d'une solution de secours.

Applications impactées secourues

- REFERENCE, EVOLUANCE GAM, EVOLUANCE GEF, CROSSWAY, PORTAIL HORIZON, QPLANNER & QDOC, MAJICS, DATAMEAL et INTRANET.
- GALAXIE et SRI.
- APIX, SYGID et VIDAL

Applications impactées non secourues

- Logiciels de GRH AGIRH, CHIMED, FOEDERIS, GESFORM, GESTOR, INDEM et PH7CUBE.
- Outils de messagerie
- PMSI Pilot, DOCUBASE, SINED, HRB2, CARDIOREPORT, MO-ARCHIVES, VISUAL ACCESS, GENSOURCE, ARMURE-GESSTOCK, LYMHOE-HLA.
- Espaces partagés et espaces de stockage des dictées numériques.
- Espace de stockage SCANBAC
- Alimentation en "Identités et Mouvements Patients" des applications DATAMEAL et QP/QD.
- Lien entre le logiciel QDOC et le PACS d'IMAGERIE.

Nous vous tiendrons informés, via le site INTRANET du déroulement des opérations.

Merci de votre attention.

Bonne Réception.

La DSIS

Figure 26 – Pertes SAN du 16 juin 2010

Le document ci-dessus, est un extrait du message diffusé par email à tout chu lors de la panne SAN du 16 juin 2010. Ce jour l'impact sur les logiciels métiers avait été étudié.

Aujourd'hui, les clusters Unix et Linux ne détectent pas convenablement les pertes SAN. En effet une partie du système étant en mémoire, la machine même sans disque dur reste moribonde et continue de donner signe de vie (ping, ssh ..). Le nœud cluster ne détectant pas la perte du heartbeat, la bascule cluster ne se fait pas.

Les clusters Windows gèrent mieux ce type de panne, le système ayant perdu soudainement son disque dur, le système crash (écran bleu), le nœud cluster détecte la perte du heartbeat, la bascule cluster s'effectue.

Il n'y a pas de perte de données. Les données critiques sont répliquées et les sauvegardes doivent assurer ce scénario de pannes.

La sauvegarde de type Disaster Recovery n'est assurée que pour les OS AIX et les OS Windows Serveur. L'outil IBM cd recorder permet la sauvegarde DR des AIX, et les sauvegardes des OS Windows2003 sont effectuées par le bais d'un module Data Protector, le logiciel de sauvegarde utilisé par la DSIS.

C - Perte d'un des châssis lames incident électrique

Dans ce chapitre je réalise un exemple d'analyse de conséquences et d'impacts à la date du 11 février 2011, sur un périmètre défini des serveurs. Ce type d'analyse permet de réaliser un « snap » de l'état des architectures à un instant donné. Etant donnée la rapidité de l'évolution et des mises à jour systèmes et applicatifs, les résultats de ce type d'analyse sont rapidement périmés.

Exemple d'analyse : Perte du châssis HP du bâtiment 1

L'ensemble des machines virtuelles n'est pas secouru. Il n'y a pas de système de cluster pour ce type de machine. Aujourd'hui lors d'une panne physique d'une des lames, les machines sont transférées manuellement sur une lame dédiée au test (1 par châssis). Cela implique plusieurs manipulations : changement de Vlan (équipe réseaux), changement de la carte réseau virtuelle (modification de l'adresse Mac par l'équipe système), modification des disques SAN par l'équipe système ce qui équivaut au minimum à 30 minutes selon la disponibilité des équipes. Bien évidemment ce scénario de reprise n'est valable que pour la panne d'une seule lame. Au delà de la perte de 2 lames, un choix devra être pris par la direction concernant la priorisation des applications à relancer.

Srv1-1 : Serveurs virtuels VS-APP1-2-3-4-12

Conséquence applicative

Machines Virtuelles	Applicatifs	Degrés de Criticité
VS-APP1	MO ARCHIVES	3
VS-APP2	VISUAL-WEB	1
VS-APP3	ARMURE – GESSTOCK	1
VS-APP3	GENSOURCE	2
VS-APP4	URQUAL ADULTE	4
VS-APP4	URQUAL ADULTE – Communications Identités & Actes	4
VS-APP12	HLA Interface Identités & Mouvements	2
VS-APP12	HLA	2
VS-APP12	SINED - Administration	3

Tableau 1 – Conséquence applicative perte lame 1 châssis 1

Selon la survenance de la panne, l'impact sur les métiers peut être significatif. Il n'existe pas de secours automatique de type cluster pour les applications SINED et Mo Archives.

Les impacts sur les services d'urgences sont moindres, étant donné que les applications des urgences sont réparties sur 2 serveurs. Le second serveur est une machine virtuelle installée physiquement dans le bâtiment 5.

SRV1-2 : Arrêt du logiciel LiveBackup

La conséquence est l'arrêt du logiciel Livebakup, Livebakup est le logiciel de sauvegarde de données des postes clients.

SRV1-3, SRV1-6 et SRV1-13 : Arrêt du serveur TSE Obelix

Il y a un impact considérable sur les postes clients fins et donc sur une partie des services critiques de l'hôpital (Carhaix, Cardiologie …) . Etant donné que la ferme des clients fins restante ne pourra pas supporter la connexion de l'ensemble des clients fins un certain nombre de postes clients ne pourra plus se connecter. L'impact au niveau des services sera lié à la période de la journée à laquelle la panne survient.

SRV1-4 : Arrêt des serveurs virtuels de supervision

L'impact est uniquement sur les consoles de supervisons destinées aux personnes de la DSIS.

SRV1-5 : Arrêt du serveur HEO-HCF

Cette machine héberge exclusivement l'application de formulaire HEO, il n'y a pas d'impact direct sur les métiers.

SRV1-7 : Arrêt de serveur EAI IPS

Ce serveur est en cluster Red Hat. La bascule des applications s'effectue donc sur le cluster de secours.

L'impact se limite au temps de la bascule de l'application, inférieur à 5 minutes.

SRV1-8 : Serveur hébergeant des applications de test.

SRV1-9 : Il s'agit du contrôleur de domaine principal et serveur DHCP, le contrôleur secondaire de domaine prend le relais automatiquement, par contre, il n'y a pas de reprise automatique du serveur DHCP.

Selon la survenance de la panne, l'impact sur les métiers peut être important. En effet, selon l'heure et le jour de la survenance de la panne, la reprise s'effectuera plus ou moins rapidement, cela dépend de la présence ou non d'un administrateur Windows. La conséquence de la perte du serveur dhcp est que tout nouveau client ne pourra se connecter au domaine.

SRV1-10 : Serveurs virtuels VS-APP5-6-11 VS-1-2

Machines Virtuelles	Applicatifs	Degrés de Criticité
VS-APP5	DATAMEAL – identités & mouvements	2
VS-APP5	Basculement Urgences --> Externes	2
VS-APP5	SINED - Appli	3
VS-APP5	traitement d'intégration SINED avec le SIH	3
VS-APP5	Interface gestion des droits HEO	2
VS-APP5	CORA_IN – EAI	2
VS-APP5	MAJ-référentiel-médecins	2
VS-APP6	Serveur de licence QP/QD (secondaire)	3
VS-APP6	CARDIOREPORT	2
VS-APP6	CORA – Interface Actes	2
VS-APP6	Interface-GE	3
VS-APP11	Antares	2
VS-COM1	PROCEDURE DEGRADEE IPS	2
VS-COM1	DOCUBASE	1
VS-COM2	QP/QD Interfaces d'intégration avec le PACS	3
VS-COM2	URQUAL ADULTES - RPU vers URQUAL BZH	1

Tableau 2 – Conséquence applicative perte lame 10 châssis 1

Selon le temps de remise en service, l'impact est limité. Au delà d'une heure d'arrêt, les conséquences sur les services sont importantes.

D - Perte totale d'une des salles informatiques par incendie ou inondation

Au vue des analyses précédentes, il est certain que la perte d'une des salles informatiques aurait des répercutions considérables sur l'ensemble du SI et donc sur un nombre important de services. La remise en service même dégradé de certains logiciels prendrait quelques heures voire quelques jours selon la disponibilité du personnel de la DSIS, des prestataires et du matériel fournisseur.

E - Infection virale de plus de 100 postes clients

L'infection virale de plus d'une centaine de postes informatiques aurait un impact fort dans les services de l'hôpital. En 2010 un cas comparable c'est produit au CHRU de Brest. La DSIS a dû faire face à un phénomène de faux positifs, c'est à dire que le logiciel antivirus du CHRU a détecté un fichier contaminé par un virus, or celui-ci était sain. Le logiciel antivirus présent sur les postes clients a supprimé un fichier système sur une grande partie du parc CHRU. La suppression de ce fichier système a causé l'arrêt brutal des machines et l'impossibilité de redémarrer le système d'exploitation. Heureusement, le phénomène à été rapporté rapidement aux administrateurs en charge du logiciel antivirus qui ont pu stopper la propagation de ce phénomène rapidement. Il y a eu 303 postes touchés.

Ci-dessous un extrait du mail de synthèse rédigé par le responsable technique DSIS au CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques) et au COSSI (Centre opérationnel de la sécurité des systèmes d'information).

De : owner-tout-dsis@mail.chu-brest.fr [mailto:owner-tout-dsis@mail.chu-brest.fr]

De la part de LE BARS RAYMOND
Envoyé : jeudi 22 avril 2010 19:31
À : CERTA-svp@certa.ssi.gouv.fr
Cc : cossi@ssi.gouv.fr; tout-dsis@chu-brest.fr
Objet : tout-dsis Thread-Index: AcriQZ4EVDPrVN4RRS6wAAlqGeetsA==

Bonjour,

Le CHRU de BREST a rencontré le problème énoncé dans la COM-003. Historique et état des lieux pour les 3000 postes pouvant être concernés :

21/04/2010 vers 16h30, de nombreux PC sont touchés et l'alerte est prise en compte rapidement par la Direction des Systèmes d'Informations et de Santé (DSIS) du CHRU.

1. Vers 17H : Avertissement aux utilisateurs par intranet et pop up d'éteindre le maximum de poste si pas d'usage, de le débrancher du réseau si possible dans le cas contraire.
2. Vers 17 H : Après recherche, élaboration en interne de la solution technique pour remettre en service les PC "Infectés" par le VIRUS.
3. Vers 17H15 : Le SAMU est isolé du reste du réseau CHRU.
4. Vers 18H30 : Décision prise de bloquer la diffusion de la base "DAT 5958". Confirmation par le commercial de McAfee d'un problème de faux positif. Impossibilité d'opérer un retour arrière pour l'ensemble des postes vers la base "DAT 5957" de manière automatique
5. Vers 19H30 : Décision d'un retour arrière de manière manuel et de vérifications des postes pour les services les plus sensibles - SAMU, URGENCES Adultes, Urgences Pédiatriques, Réanimation, Pole Biologie - une centaine de postes sont traités et reprennent un travail. normal (71 PC "Prioritaires/Stratégiques" ont été traités préventivement, pas de problème rencontré) fin de l'opération vers 2h30 le 22/04 - problématique d'accès aux box occupés des urgences.
6. Vers 21H : Le patch pour la base "DAT 5958" est installé sur la console pour être "poussé" sur l'ensemble des postes.
7. Vers 22H30 : Des messages sont transmis aux utilisateurs pour remise en route des postes avec consignes de faire circuler l'information.
8. 5 agents équivalent temps plein le 21/04 pour Organisation/Interventions.

22/04/2010

1. Vers 3H : Décision pour les agents présents d'arrêter les opérations jusqu'au lendemain matin 8H. Les statistiques McAfee ne sont pas assez fiables pour cerner l'ampleur du problème et continuer les actions. Information est faite aux utilisateurs de signaler les problèmes au Centre d'Appel et d'Assistance de la DSIS (CAA)
2. 8H : Reprise de l'activité

a. Mise en place de la cellule de crise et de coordination - information à un maximum du personnel de la DSIS sur les actions correctives à mener.
b. Début d'enregistrement des appels utilisateurs par le Centre d'Appel et d'Assistance de la DSIS, (3 personnes).
c. Installation base "DAT 5959" sur console pour être "poussée" vers tous les postes

3. 8H30 : Départ des agents dans les services de l'Hôpital, avec répartition par établissements - bâtiments et première liste de PC à corriger manuellement.
4. Vers 9hH0 : Information et transmission de la solution aux agents du Biomédical du CHRU pour actions sur les postes biomédicaux rencontrant le problème.
5. Tout au long de la journée gestion de la crise par le CAA (enregistrement des appels, information), la cellule de crise (distribution des appels, gestion des priorités, clôture, enregistrement des demandes directes pour exhaustivité) et les agents du terrain (correction, prise en compte des demandes directes, gestion des priorités interne service, transmission)
6. 17H30 : Point :

d. 20 agents équivalents temps plein le 22/04 pour Organisation/Suivi/Interventions.
e. 303 postes touchés,
f. 71 traités en préventions,
g. Total des actions 303+71=374,
h. Fiches closes 256,
i. 18 fiches non closes (absence, accès locaux, problèmes particuliers)
j. Décision d'arrêter les actions pour la journée

Suite

1. Finir de clore les incidents.
2. Point de vigilance le lundi 26/04, reprise de travail après congés.
3. Travailler avec McAfee sur une meilleure information pour anticipation et préparation actions correctives.
4. …

F - Défaillances fournisseurs de services : EDF, SFR

Malheureusement, l'ensemble des services de l'hôpital ne bénéficie pas de prises de courants secourues. Les sites les moins récents comme le site de Morvan ou Ponchelet, ont certains services qui ne possèdent pas de prises de courants secourues. Par conséquence, à chaque coupure électrique, ces services se retrouvent sans électricité et donc sans système d'information.

Une cartographie précise doit être réalisée par les services techniques et transmise à la DSIS. Un point avec les services techniques sur cette problématique est planifié courant août.

Le Bips Breizh IP Santé est le réseau haut et très haut débit de la communauté de santé bretonne, publique comme privée. En 2009, avec la fin du marché MEGALIS II pour la Santé, la communauté de santé bretonne a souhaité assurer par ses propres moyens la continuité de ses raccordements IP ainsi que ses services de visioconférence. Depuis décembre 2009, les entreprises SFR et NOVASIGHT fournissent, respectivement, les services de connectivité IP et d'audio/visioconférence à la communauté de santé bretonne. Le BIPS dote la totalité de la communauté de santé bretonne d'une infrastructure de connectivité IP à haut et très haut débit, fiable, non bloquante et évolutive. Au CHRU de Brest, les arrivées Bips donc d'internet se font sur 2 points d'entrées différents et redondés. Malgré cela nous avons eu à déplorer 2 coupures majeures (plus d'une heure) depuis 2009.

G - Indisponibilité du personnel informatique : pandémie

Suite à la pandémie de grippe H1N1 en 2010, des recommandations ont été transmises depuis le ministère de la santé et du travail et diffusées à l'ensemble des services de l'hôpital. Une campagne de sensibilisation par des affiches a été menée. Par contre aucun plan de télétravail n'a à ce jour été étudié.

4.1.4 SYNTHESE ET PLAN D'ACTION ANALYSE GMSIH

Liste des actions à privilégier après l'analyse GMSIH :

- Ecriture et mise en œuvre d'une politique de sécurité du système d'information.
- Classification des ressources
- Réaction aux incidents et aux défauts de fonctionnement
- Sensibilisation

4.1.4.1 ECRITURE ET MISE EN ŒUVRE D'UNE POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION (PSSI)

Depuis septembre 2010 je fais partie d'un groupe de travail piloté par le GCS. Les membres du groupe sont issus de différents établissements de santé de Bretagne : Rennes, Saint Brieuc, Quimper, Lorient …. . L'une des missions de ce groupe est de rédiger un modèle de PSSI cohérent. La PSSI est l'expression de l'engagement d'un organisme dans une démarche sécurité de ses systèmes d'information. Il est recommandé, voire exigé, par les instances ou les normes internationales : ANSSI, ISO27001, RGS (Référentiel Général de Sécurité).

Ce document est propre à chaque organisme, donc à chaque établissement de santé. Cependant il se base sur des modèles proposés par divers structures du monde de la santé :

- Le GMSIH a produit en 2005 une PGSSI, Politique Globale de Sécurité des Systèmes d'Information, comme modèle à destination des établissements de santé français.
- L'ASIP, suite à la réorganisation de 2009 qui a vu disparaitre le GMSIH, reprend ce document pour une nouvelle version, prévue pour 2012.
- Le Ministère de la santé au travers de la PMSSI (Ref : Figure 2, chapitre 2.3).

La politique de sécurité des systèmes d'information d'un établissement est un document stratégique. Elle reflète la vision de la direction de l'établissement vis-à-vis de la sécurité de ses systèmes d'information. Elle présente les objectifs qu'elle s'est fixés, les moyens qu'elle apporte ou qu'elle prévoit d'apporter pour atteindre ces objectifs. Ces moyens sont humains – définition des rôles et responsabilités et création des postes associés - et organisationnels, par la mise en place de comités de suivi et de pilotage et d'instances de contrôles et d'audits permettant la gestion de cette sécurité.

Les domaines de sécurité abordés dans une politique de sécurité sont les suivants :

- Politique de sécurité
- Management de la sécurité
- Inventaire et classification des ressources
- Sécurité et ressources humaines
- Sécurité physique et sécurité de l'environnement
- Exploitation informatique et gestion des réseaux
- Contrôle d'accès logique
- Développement et maintenance des applications et systèmes
- Gestion des incidents de sécurité
- Gestion de la continuité
- Respect de la réglementation externe et interne

Chaque établissement de santé est maitre de la rédaction de sa politique de sécurité et du choix de la structure documentaire. L'objectif d'une politique de sécurité est de couvrir tous les domaines et d'avoir défini des règles de sécurité couvrant l'ensemble des risques et répondant aux objectifs de sécurité des systèmes d'information de l'établissement. Je suis chargé par ma direction de rédiger et de mettre en œuvre cette politique, cette politique de sécurité du système d'information devra être validée et signée par la direction générale de CHRU de Brest.

4.1.4.2 CLASSIFICATION DES RESSOURCES

J'ai entrepris et réalisé la classification des ressources pour grande partie lors de mon analyse du contexte et de ma cartographie du SI (voir chapitre 4.1.2). Je suis en charge de garder ce document à jour.

4.1.4.3 REACTION AUX INCIDENTS ET AU DEFAUT DE FONCTIONNEMENT

Suite à l'analyse du GMSIH, j'ai modifié l'ordre du jour de chaque réunion de travail du groupe de sécurité qui se réunit une fois par mois pour traiter de la SSI. Pour chaque incident, une main courante est rédigée par les personnes concernées par l'incident. Dorénavant, à chaque début de séance, un débriefing est fait sur les incidents du mois et les mains courantes sont reprises, les incidents analysés et des contremesures sont proposées si nécessaire. De plus, des scénarii de test de bascule cluster ou de restauration sont planifiés et réalisés tous les mois. Je suis en charge de piloter ces tests en collaboration avec les administrateurs systèmes, administrateurs de bases de données (DBA) et les responsables du groupe métier impactés par les tests de continuité.

4.1.4.4 SENSIBILISATION

Le 23 juin 2011, j'ai pris rendez-vous avec le service de communication de l'hôpital, afin de lui présenter et proposer une campagne de sensibilisation sur la sécurité informatique. Nous avons convenu de la mise en œuvre d'une compagne de sécurité au travers différents supports : magazine interne (Pulsation), site intranet, affiche dans les services, dépliant dans l'enveloppe du bulletin de salaire, écrans de veille sur une grande partie des pc. Cette campagne débutera en septembre.

Un logiciel spécialisé dans la sensibilisation de la sécurité informatique va être acheté par le CHRU. Cette application est inscrite dans le lot 4 du CCTP SSI d'UNI-HA (Union des Hôpitaux pour les Achats) auquel le CHRU a adhéré.

Deux personnes du groupe de la Centrale d'appels dont j'ai la responsabilité, réalisent des formations sur la bureautique tout au long de l'année. Ces formations touchant un public très large, je vais demander aux formateurs de consacrer du temps pour échanger sur la sécurité informatique et plus spécifiquement sur les procédures dégradées. A cet effet une brochure sur la thématique de la sécurité informatique va être écrite et sera remise à chaque personne présente aux formations.

4.1.5 LISTE DES ACTIONS A MENER SUITE A L'ANALYSE PCRI

4.1.5.1 MACHINES BLANCHES

Les résultats de l'analyse réalisée dans les précédents chapitres, ont été présentés au comité de pilotage. La décision du principe de machine blanche sur les machines identifiées comme critiques sera réalisée. Monsieur Pallier en tant que responsable du groupe applications métiers en collaboration avec Jean Yves Le Henaff (Ingénieur système) sont chargés de la migration des applicatifs et de la mise en place des clusters associés. Monsieur Jacquemin, en tant que responsable du groupe technologies est chargé de l'achat des nouveaux châssis nécessaires.

Un appel d'offres a été lancé en mai 2011. La migration des applications et la « clusterisation » de celles-ci se dérouleront d'une façon échelonnée jusqu'à fin novembre 2011.

4.1.5.2 SAUVEGARDE ET DISASTER RECOVERY

J'ai demandé à ce que l'équipe sauvegarde mette en œuvre en plus des sauvegardes de fichiers, des sauvegardes de type Disaster Recovery sur l'ensemble des machines jugées critiques dans l'étude PCRI.

J'ai mené en collaboration avec Monsieur Borchtchov une des personnes en charge des sauvegardes à la DSIS, un travail sur le logiciel REAR afin de prendre en compte les machines linux. A ce jour, Red Hat préconise la réinstallation complète de la machine après perte totale d'une machine. Cela n'est pas satisfaisant. Après avoir cherché et étudié plusieurs solutions, nous avons mis en œuvre la solution libre REAR sur les machines identifiées comme critiques dans l'étude PCRI.

4.1.5.3 BOUCLE RESEAU

Afin de sécuriser au mieux l'infrastructure réseaux du CHRU, un programme d'envergure baptisé « boucle réseau » a été écrit, chiffré par l'équipe réseaux et les services techniques de l'hôpital. Ce document n'est pas à ce jour validé par la direction générale.

4.1.5.4 CLUSTER ET MACHINES VIRTUELLES

Une étude sur la virtualisation et la mise en haute disponibilité des machines virtuelles doit être réalisée par Patrick Jacquemin et son équipe avant la fin de l'année 2011. A l'issue de cette étude, un appel d'offres sera lancé et les machines virtuelles jugées critiques dans l'étude PCRI seront mises en haute disponibilité par la solution de virtualisation retenue.

4.1.5.5 TELETRAVAIL

Un appel d'offres concernant les éléments de sécurité réseaux périmètriques a été lancé en juin 2010. Les nouveaux éléments permettent de supporter la mise en place de télétravail de l'ensemble des membres de la DSIS en cas de pandémie grave au sein du service.

4.1.5.6 SECURISATION SAN

Un audit des clusters Red Hat par un prestataire de l'entreprise Red Hat a été réalisé en juin 2010 au CHRU de Brest. Lors de cette prestation l'un des points demandé et traité par le spécialiste Red Hat a été la prise en charge de perte San dans le Cluster Suite Red Hat. Des solutions ont été proposées mais aucune solution réellement fiable couvrant la perte SAN n'a été trouvée puis mise en œuvre.

4.1.6 REDACTION DU PLAN DE CONTINUITE ET DE REPRISE INFORMATIQUE

4.1.6.1 PLAN DE GESTION DE CRISE

Ce document décrit l'ensemble des acteurs et détaille leurs responsabilités. J'ai rédigé avec l'aide de Madame Cortes, l'ingénieur processus de la DSIS un document listant l'ensemble des logiciels gérés par la DSIS. Pour chaque logiciel, un référent informaticien et un co-référent est identifié.

Le même travail à été réalisé sur l'ensemble des éléments composant l'infrastructure informatique (ref chapitre 4.1.2.2 Inventaire des actifs).

Il me restera à réaliser le synoptique de la gestion de crise, de la survenance du sinistre au retour fonctionnel et technique initial. Une fois ce synoptique défini, je le ferai valider par l'équipe de pilotage projet.

4.1.6.2 PLAN DE CONTINUITE INFORMATIQUE

Ce plan décrit l'architecture informatique, il comporte les référentiels techniques.

Il se compose d'un ensemble de fiches réflexes rédigées par les référents logiciels informaticiens. Une très grande partie de ces fiches avait été rédigée lors de la mise en place d'astreintes informatiques en 2009.

4.1.6.3 PLAN DE REPRISE INFORMATIQUE

Ce document devra décrire l'organisation et les processus à mettre en œuvre pour la reprise des éléments informatiques après la survenance d'un sinistre. Un groupe de travail sera monté spécifiquement pour la rédaction de ces documents. Une fois rédigé, ce document sera validé par le comité de pilotage.

4.1.6.4 PLAN DE SAUVEGARDE

Ce document décrit les processus de sauvegarde mis en œuvre pour assurer les sauvegardes. Il contient également les procédures de restauration de chaque type de données sauvegardées. Ce document est mis à jour par l'équipe sauvegarde de la DSIS

4.1.6.5 PLAN DE TEST

Des scénarii de tests de bascule cluster ou de restauration sont planifiés et réalisés tous les mois. Je suis en charge de piloter ces tests en collaboration avec les administrateurs systèmes, administrateurs de bases de données (DBA) et les responsables du groupe métiers impactés par les tests de continuité. La description des scénarii de tests, le résultat attendu, le résultat effectif, les comptes rendus des réunions du groupe sécurité, les analyses des tests, les mains courantes sont consignés dans ce plan.

4.1.6.6 PROCEDURE DEGRADE UTILISATEUR

Ce document décrit les mesures à mettre en œuvre au niveau des services, à la survenance d'une panne, quelle qu'en soit l'origine. En annexe de ce document, on retrouve les procédures dégradées utilisateurs et fiches réflexes utilisateurs. Depuis de nombreuses années, la DSIS met en œuvre des procédures dégradées en collaboration avec des référents métiers. J'ai mené un travail de « rafraichissement » de ces procédures, certaines demandant à être mises à jour.

4.2 PLAN DE CONTINUITE D'ACTIVITE LOCAL SAMU29

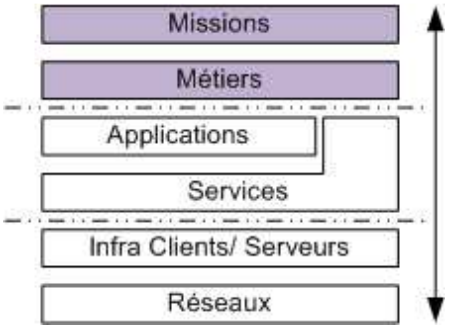
L'activité du SAMU ayant rencontré des perturbations en terme de continuité de service en juillet août 2010, ma direction a souhaité que je pilote et mette en place un plan de continuité spécifique à la mission du SAMU et cela de façon prioritaire.

4.2.1 LANCEMENT, ORGANISATION ET CONDUITE DU PROJET

Dans ce chapitre je définis dans un premier temps le contexte du projet et la démarche de ce projet. Dans la seconde partie, je décris le périmètre, et les équipes projets.

4.2.1.1 DEMARCHE ET OBJECTIF

L'une des missions primordiales de l'hôpital est le service d'aide médicale d'urgence (SAMU), le centre 15 du Finistère.



En 2009, il a été décidé de faire évoluer l'infrastructure téléphonique afin d'optimiser la prise en charge des appels.

La solution retenue est la solution Genesys de la société Nextiraone.

La nouvelle solution permet de superviser l'activité téléphonique de la salle de réception des appels "15" et d'établir des statistiques. Elle permet également de disposer d'un outil adéquat face à la gestion d'une crise sanitaire ou du déclenchement d'un plan de secours.

L'objectif qui m'a été confié est de mettre en œuvre un plan de continuité local du SAMU29.

En juin 2010 le service du SAMU 29 a changé de locaux, et a aménagé dans le nouveau pôle au niveau des urgences adultes.

4.2.1.2 COMPOSITION DE L'EQUIPE PROJET

L'équipe projet PCA Local SAMU29

Cette équipe est composée de :

- Docteur Pondaven, responsable du pole SAMU du Finistère
- Docteur L'Azou, médecin régulateur
- Docteur Penarguear, médecin régulateur
- Vanessa Maze, permanencière
- Jean Claude Derrien, Responsable téléphonie des services techniques
- Moi-même en tant que responsable projet

4.2.1.3 PLANNING ET PLANS D'ACTIONS

	A	B	C
1			
2	Plan d'action pour la mise en place du Plan de continuité SAMU		
3			
4	*Phase*	*Fiche de l'action (objet)*	*Objectifs de l'ac*
5	1 Lancement,organisation et conduite de projet	La démarche	Définition de la démarche
6		Engagement de la Direction	- Valider le projet de Plan de Continuité local Samu
7		Objectif du Plan de Continuité et de Reprise Informatique	- Valider les objectifs, le périmètres, le planning e place du PCA Samu
8		Composition de l'équipe projet	- Mise en place d'une équipe projet
9	2 Analyse du contexte et Cartographie du SI	Fonctionnalité	
10			
11			
12		Solution existante	
13			
14		Les acteurs	
15			
16			
17			
18	3 Identification des menaces et des risques	Analyse des risques	Analyse des risques
19			- Identifier les risques et menaces potentiel et leu
20			Valider les scénarii de risque par le Comité de pilo
21		Analyse d'impact	- Etudier l'ensemble des processus et leurs beso
22			Estimation des durées d'interruption maximales ac
23			- Evaluer leur criticité des processus, les DIMA et normale suite à un sinistre

Figure 27 – extrait planning projet PCA SAMU

		Nom	Durée	Début	Fin
14		⊟AG-29_SAMU29_Architecture_Serveurs_	110 jours	23/06/10 08:00	23/11/10 17:00
15	✔	Commande EMC	1 jour	23/06/10 08:00	23/06/10 17:00
16	✔	Livraison EMC	14 jours	24/06/10 08:00	13/07/10 17:00
17	✔	Commande presta EMC	1 jour	01/07/10 08:00	01/07/10 17:00
18	✔	Commande Sun	1 jour	09/08/10 08:00	09/08/10 17:00
19	✔	Livraison Sun	14 jours	10/08/10 08:00	27/08/10 17:00
20		Préparation serveurs Sun	3 jours	11/10/10 08:00	13/10/10 17:00
21		Commande PC vcenter	1 jour	07/10/10 08:00	07/10/10 17:00
22		Livraison des PC vcenter	9 jours	08/10/10 08:00	20/10/10 17:00
23		Préparation PC vcenter	2 jours	25/10/10 08:00	26/10/10 17:00
24		Livraison client	5 jours	27/10/10 08:00	02/11/10 17:00
25		Fourniture du lien fibre	1 jour	12/11/10 08:00	12/11/10 17:00
26		Déploiement du matériel	5 jours	15/11/10 08:00	19/11/10 17:00
27		Migration	1 jour	23/11/10 08:00	23/11/10 17:00

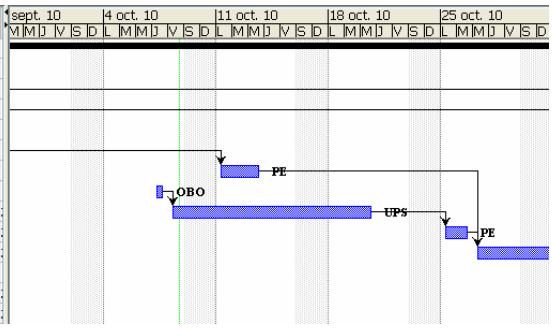


Figure 28 – extrait planning déploiement solution Appligos

4.2.2 ANALYSE DU CONTEXTE ET CARTOGRAPHIE DU SI

Le SAMU 29 a changé récemment (début d'année 2010) son infrastructure téléphonique.

Un CCTP a été publié en 2009. La nouvelle solution permet.

- Optimiser la prise en charge des appels. Objectif national de 99% de décrochés en moins de 60 secondes
- Connaître les identifiants des appels avant décroché pour prioriser leur prise en compte en fonction de leur typologie
- Assurer la prise en compte des appels téléphoniques en fonction du degré de gravité de la demande, à chacun des niveaux du cheminement de l'appel
- Sécuriser les appels entrants en cas de panne de l'autocommutateur ou de saturation par routage automatique des communications
- Superviser l'activité téléphonique de la salle de réception des appels "15" et établir des statistiques
- Disposer d'un outil adéquat face à la gestion d'une crise sanitaire ou du déclenchement d'un plan de secours
- Améliorer les conditions de travail du personnel en salle : poste de travail ergonomique et réduction des bruits

Les Fonctionnalités minimales :

- Dialogue possible avec d'autres autocommutateurs de marque différente
- Interception d'appel
- Rappel automatique sur non réponse
- Rappel du dernier numéro composé
- Conférence téléphonique
- Consultation d'un appel en attente
- Double appel
- Indicateur d'appels en attente

Gestionnaire des appels téléphoniques

- La gestion des flux : compétences spécifiques pour chaque utilisateur
- La distribution automatique des appels vers la file d'attente adaptée
- La possibilité de se mettre en attente temporaire de réception
- La reconnaissance des numéros de téléphone entrants avant le décroché (CTA--CODIS, CTA--Marine, SOS Médecins, CROSS, SMUR…)
- La présentation d''un appel téléphonique déjà reçu, vers l'utilisateur qui a traité le dossier correspondant
- La possibilité d'activer des scénarii de gestion de crise

- L'édition de tableaux et courbes statistiques
- La définition de seuils d'alertes avec déclenchement gradué d'alarme en fonction du dépassement de certains critères
- Un affichage dynamique de l'activité téléphonique du centre d'appels en temps réel sur support écrans muraux,

En septembre 2009, après dépouillement des différents appels d'offres, le choix commun SAMU, services techniques, DSIS, s'est porté sur la solution proposée par Nextiraone

Descriptif solution Nextiraone :

- Un socle PBX s'appuyant sur un équipement ALCATEL-LUCENT
- La partie routage intelligent des appels traités par GENESYS
- Un bandeau informatique pour visualiser et dispatcher les appels (mediQ)
- Enregistrement des conversations réalisé avec ASSMANN
- La partie automate d'appels avec NEWVOICE,
- Cette solution, nativement multi-sites, très simple à mettre en place afin de respecter des choix locaux, peut ensuite être répartie sur plusieurs SAMU/Centre 15 et ainsi bénéficier de la mutualisation des ressources régionales

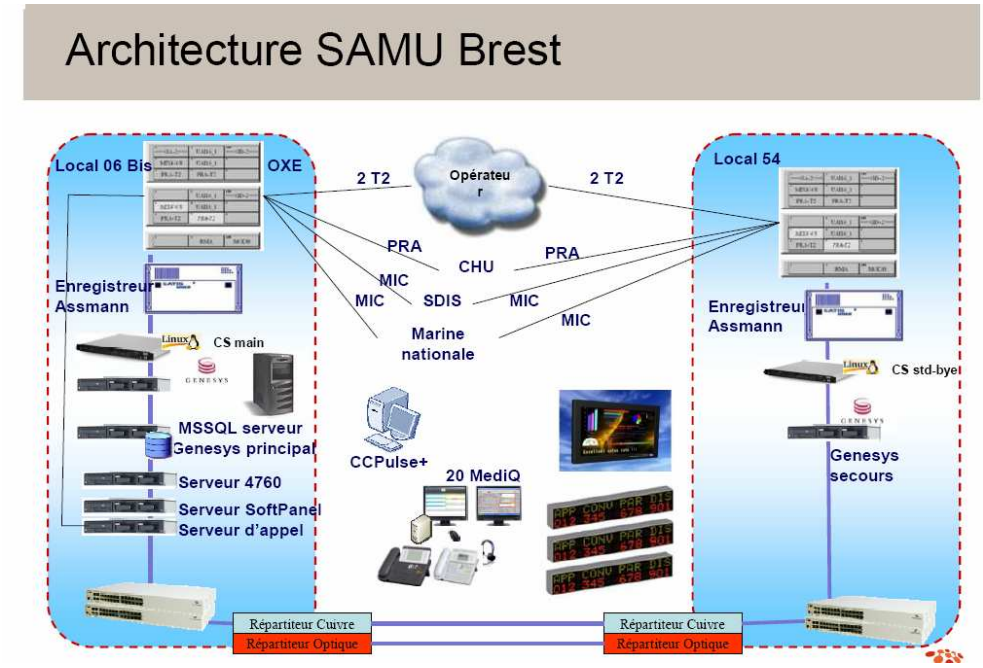


Figure 29 – extrait du dossier de spécification fonctionnel Nextiraone

La solution Genesys permet le traitement des appels entrants. La solution WallBoard Manager permet l'affichage de statistique en temps réel sur des écrans LCD en salle de régulation.

La gestion des appels ambulanciers privés s'effectue par le biais du logiciel SCR, il s'agit d'une application web.

Les enregistreurs Assman sont directement raccordés aux autocommutateurs, ils enregistrent les conversations téléphoniques du 15. L'enregistrement des appels 15 est une obligation légale.

La gestion des dossiers patients est assurée par la solution Applisamu de la société Appligos.

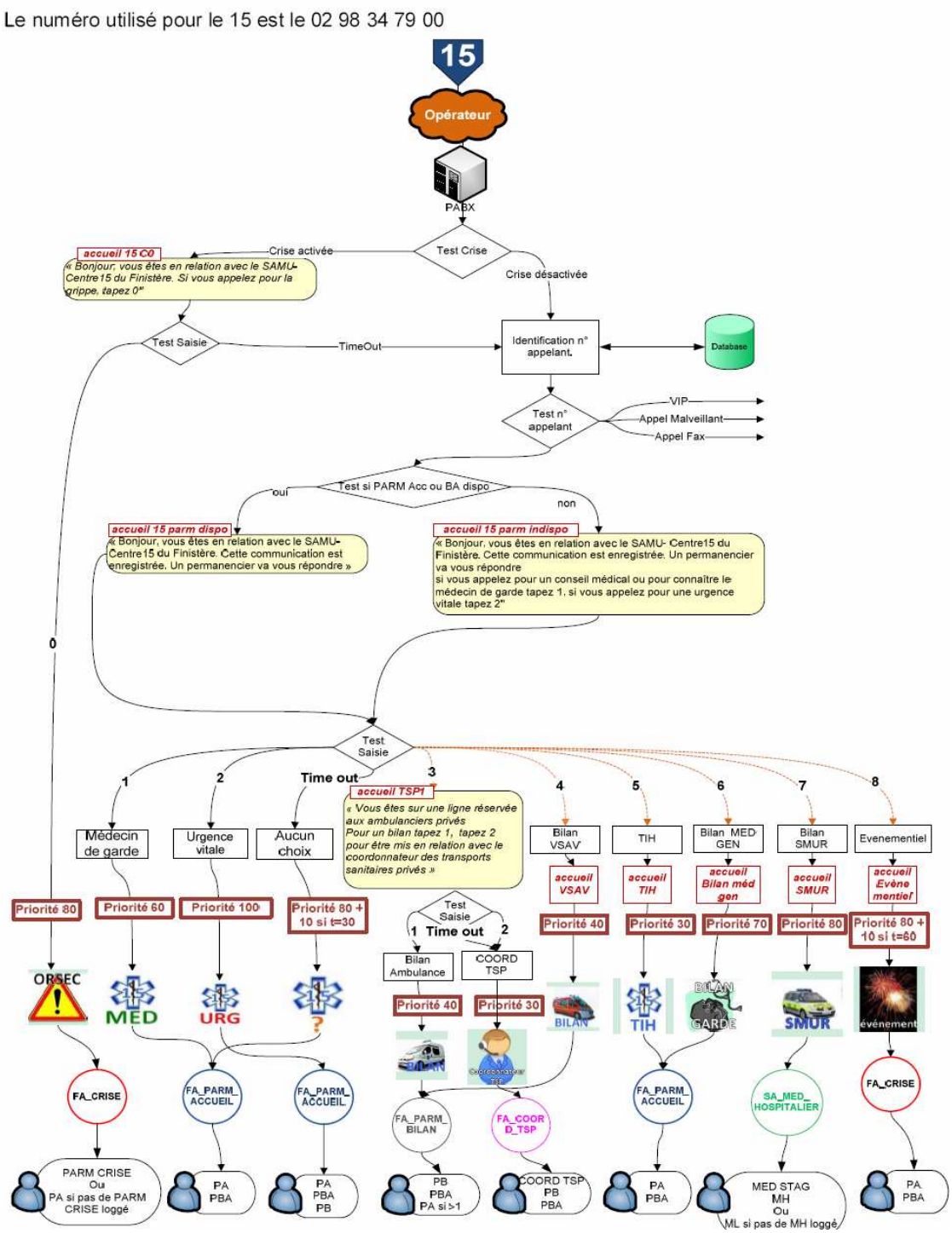


Figure 30 – extrait du dossier de spécification fonctionnel Nextiraone

Photo 1 – Photo d'un poste de régulation Samu 29

4.2.4 LES ACTEURS

DSIS : La direction des systèmes d'information de santé, est le service interne qui gère l'ensemble du réseau informatique et met à disposition les postes clients du SAMU.

Services Techniques : Le service technique du CHRU, est le service qui gère l'ensemble du réseau téléphonique.

La société Appligos : Cette société a en charge la maintenance et le suivi applicatif du logiciel APPLISAMU

La société Nextiraone : Cette société a en charge la maintenance et le suivi applicatif du logiciel MediQ de téléphonie.

La société SCR : Cette société est l'interlocutrice privilégiée pour tout ce qui concerne SCR'URGENCES – Déclenchement (gestion des appels d'ambulanciers privés). Elle a en charge La maintenance et le suivi applicatif du logiciel SCR

La société Assman : Cette société à en charge de la maintenance des enregistreurs d'appels.

4.2.5 ANALYSE DES RISQUES

Suite à des perturbations en terme de continuité de service en juillet-août 2010, ma direction a souhaité que je pilote et mette en place un plan de continuité spécifique à la mission du SAMU et cela de façon prioritaire. Une analyse des risques avec la méthode SHAM à été menée et les menaces et scénarii de sinistres énumérés.

Menaces

Sinistres physiques affectant un bâtiment (locaux) : incendie, inondation,
Défaillance techniques
Indisponibilité du personnel informatique : pandémie
Défaillance fournisseurs de services : SFR, EDF
Attaques virales

Scénarii de sinistres retenus

1) Perte d'un élément réseau
2) Perte d'un autocommutateur téléphonique
3) Perte d'un serveur applicatif
4) Perte totale d'une des salles techniques
5) Perte d'accès Internet
6) Attaques virales

Après étude des problèmes techniques rencontrés courant juillet aout 2010, les administrateurs Windows de la DSIS ont trouvé que le problème venait d'une saturation des cartes réseaux de la machine physique qui héberge les machines virtuelles HyperV Nextiraone. La solution a été l'installation d'un patch OS sur le serveur HyperV.

Au delà du simple problème technique, cet épisode a permis de mettre en lumière un réel problème organisationnel et de pilotage en temps de crise. En effet étant donné le nombre d'acteurs : DSIS, Services technique du CHRU, Nextiraone, Appligos, SCR, Assman et l'interopérabilité des différentes infrastructures gérées par ces acteurs, à la survenance d'une panne il est très difficile de déterminer la responsabilité de chacun.

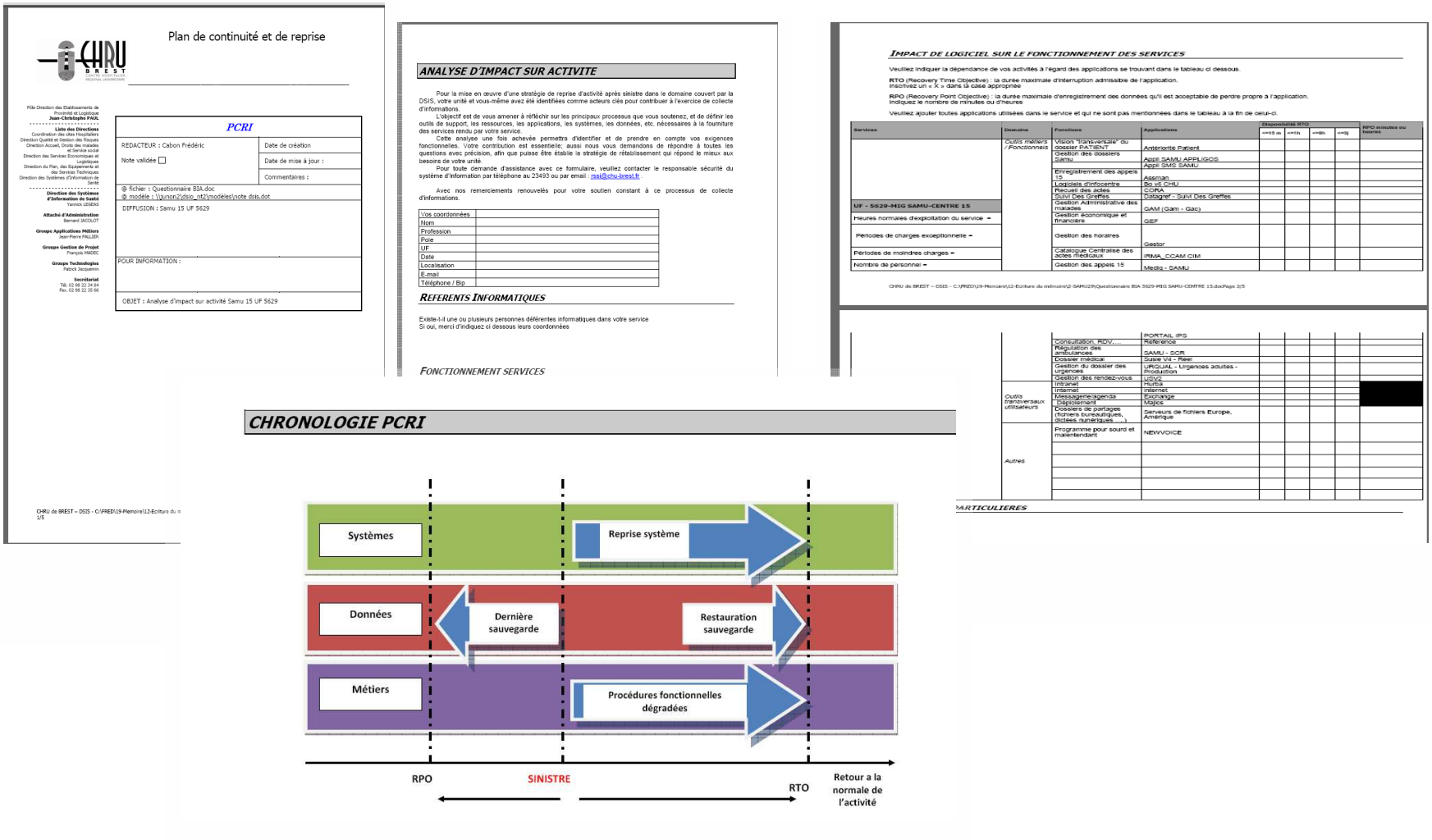
Ma première décision a été de dresser un document indiquant le périmètre de responsabilité de chacun des acteurs. Afin d'améliorer la communication entre les acteurs, j'ai mis à disposition, un tableau regroupant les caractéristiques de chaque élément composant l'infrastructure et leur correspondance dans les différentes spécialités. En effet, un informaticien pour identifier une poste SAMU, va parler en adresse IP, un technicien du service technique lui parlera en n° de téléphone alors qu'une personne de la régulation, va parler en nom d'emplacement. (Voir tableau ci dessous)

Emplacement	Numéro	Nom_Tel	IP Phone	Nom_Pc
B2	40808	TB2	10.106.10.103	chu3104
B6	40812	TB6	10.106.10.104	chu3114
C2	40814	TC2	10.106.10.105	chu3101
C3	40815	TC3	10.106.10.106	chu3100
D3	40819	TD3	poste numérique	chu3113
D4	40820	TD4	10.106.10.107	chu3111
E1	40821	TE1	poste numérique	chu3107
E5	40825	TE5	10.106.10.109	chu3125
			poste	

Tableau 3 – extrait du tableau de correspondance

4.2.6 ANALYSE D'IMPACT

Pour réaliser l'analyse d'impact, un questionnaire BIA (Bilan d'Impact sur l'Activité), a été transmis aux membres de l'équipe projet. Au retour de l'ensemble des formulaires, un débriefing a été réalisé et le tableau d'impact logiciel sur le fonctionnement du service SAMU a été réalisé.



Figures 31 – Questionnaire BIA

4.2.7 SYNTHESE DE L'ANALYSE D'IMPACT

Fonctionnement du service

Les heures normales d'exploitation du service sont de 24/24, 7 jours sur 7. Les périodes de charges exceptionnelles sont

- Les fériés : jour de l'an, lundi de Pâques, 14 juillet, Noël, lundi de Pentecôte, 15 août puis 1er mai… jusqu'à 4000 communications téléphoniques /24h
- Les dimanches jusqu'à 3000 communications
- Les samedis jusqu'à 2500 communications – 1600 communications en jour de semaine

Il y a jusqu'à 400 communications/heure en fin de matinée des jours fériés – 200/h en fin de matinée les dimanches 100/h dans l'après midi les samedis et le pic de 70 à 90/h peut être atteint en milieu de soirée en semaine.

Les périodes de moindre charge sont essentiellement en semaine et en période nocturne. L'activité peut descendre jusqu'à 10 communications/h entre 3h et 5h du matin. En période de semaine l'activité la plus basse constatée se situe en début d'après midi (cela peut descendre à 20 communications/h entre 14h et 15h) puis en milieu de matinée (peut descendre à 25 communications/h).

Le **nombre minimal de personnel** pour assurer un fonctionnement aux heures normales du service est en semaine :

- Journée 3 à 5 PARM (permanencier auxiliaire de régulation médicale), 2 médecins régulateurs
- Soirée 4 PARM, 3 médecins régulateurs
- Nuit 3 PARM, 2 médecins régulateurs
- Samedi journée 4 à 6 PARM, 3 à 4 médecins régulateurs
- Dimanche journée 5 à 8 PARM, 3 à 4 médecins régulateurs

Le **nombre minimal de personnel** pour assurer un fonctionnement en périodes de charges exceptionnelles est :

- Journée 5 à 8 PARM, 4 médecins régulateurs
- Soirée 5 PARM, 4 médecins régulateurs
- Nuit 4 à 5 PARM, 2/3 médecins régulateurs

Impact de logiciel sur le fonctionnement des services

Le RTO pour « Recovery Point Objective », désigne la durée maximale d'interruption admissible vis-à-vis de l'utilisateur métier, c'est-à-dire le temps maximal acceptable, pendant lequel une ressource informatique n'est plus fonctionnelle.

Le RPO « Recovery Time Objective », est la durée maximale d'enregistrement des données qu'il est acceptable de perdre. Cet indicateur permet de juger au mieux des sauvegardes à mettre en œuvre

Domaine	Fonctions	Applications	Disponibilité RTO				RPO minutes ou heures
			<=15 m	<=1h	<=8h	<=3j	
Outils métiers / Fonctionnels	Vision "transversale" du dossier PATIENT	Antériorité Patient					
	Gestion des dossiers Samu	Appli SAMU APPLIGOS					0
	Enregistrement des appels 15	Assman					0
	Logiciels d'infocentre	Bo v6 CHU					
	Recueil des actes	CORA					
	Suivi Des Greffes	Datagref - Suivi Des Greffes					
	Gestion Administrative des malades	GAM (Gam - Gac)					
	Gestion économique et financière	GEF					
	Gestion des horaires	Gestor					
	Catalogue Centralisé des actes médicaux	IRMA_CCAM CIM					
	Gestion des appels 15	Mediq - SAMU					0
	Gestion du dossier patient	PORTAIL IPS					
	Consultation, RDV….	Reference					
	Régulation des ambulances	SAMU - SCR					24h

	Dossier médical	Susie V4 - Reel					
	Gestion du dossier des urgences	URQUAL - Urgences adultes - Production					
	Gestion des rendez-vous	USV2					
Outils transversaux utilisateurs	Intranet	Hurba					
	Internet	Internet					
	Messagerie/agenda	Exchange					
	Dossiers de partage (fichiers bureautiques, dictées numériques ….)	Serveurs de fichiers Europe, Amérique					
	Programme pour sourd et malentendant	Appli SMS SAMU/NEWVOICE					

Tableau 4 – Tableau de synthèse BIA SAMU

4.2.8 SOLUTIONS TECHNIQUES MISES EN ŒUVRE

4.2.8.1 SALLE BLANCHE

Au vu des scénarii de pannes, le principe de la salle blanche a été choisi. Les salles serveurs sont constituées de 2 locaux techniques. Le site principal est situé en annexe de la salle de régulation au pôle urgence niveau 0, cette salle est toujours fermée à clés. La salle de secours, le local 54, est située au niveau -1 du pole 3. Les 2 salles possèdent une climatisation adaptée, et des prises normales et redondées.

4.2.8.2 CONTINUITES TELEPHONIQUES

La solution téléphonique se compose de deux autocommutateurs principaux (PABX) et d'un autocommutateur de secours. Le premier autocommutateur gère 1 ligne entrant et sortant du 15 et 2 lignes internes au réseau téléphonique du CHRU. Le deuxième autocommutateur gère 2 lignes entrant et sortant du 15 et 1 ligne directe au réseau téléphonique de la marine. L'autocommutateur de secours est raccordé à 1 ligne 15.

La solution de gestion téléphonique Genesys, est installée sur les serveurs :

- srv-samu-genbdd serveur de base de données
- srv-samu-gen01 serveur applicatif principal
- srv-samu-gen02 serveur applicatif de secours

Le système de reprise est un mode de cluster applicatif actif-passif.

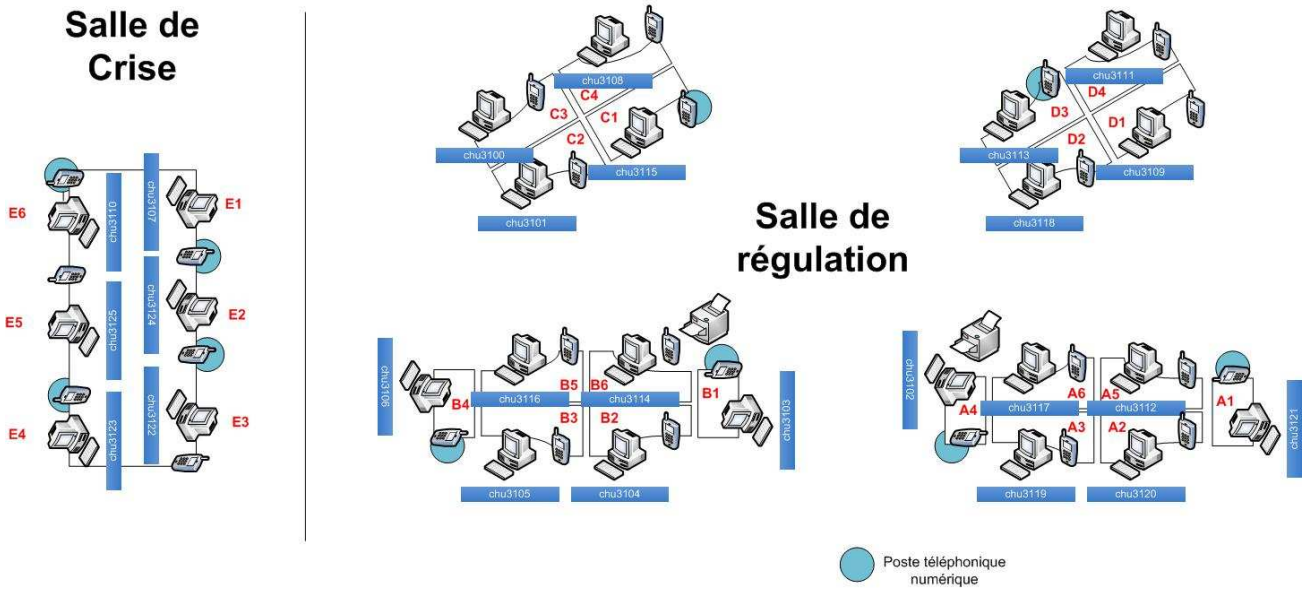
Le serveur de base de données ne fait pas partie d'un mécanisme de haute disponibilité, en cas de coupure de la base, les statistiques des appels sont stockées en local sur les postes clients. Une resynchronisation s'effectue lors de la relance de la base avec les postes clients.

4.2.8.3 CONTINUITE DES POSTES CLIENTS

La salle de régulation est composée de 20 emplacements. Le brassage informatique et téléphonique est effectué afin de pallier à la perte d'un cœur de réseau, la moitié des postes est brassée directement sur le SRI10 et l'autre sur le SRI11. Le nombre important de postes clients permet une souplesse d'intervention lors d'une panne sur un des postes.

Par emplacement est installé un ordinateur, et un élément téléphonique IP ou numérique. La salle de crise est composée de 6 emplacements.

Parmi les 26 emplacements, il y a 10 postes numériques (non tout IP), ces postes permettent de couvrir une panne globale du réseau IP.

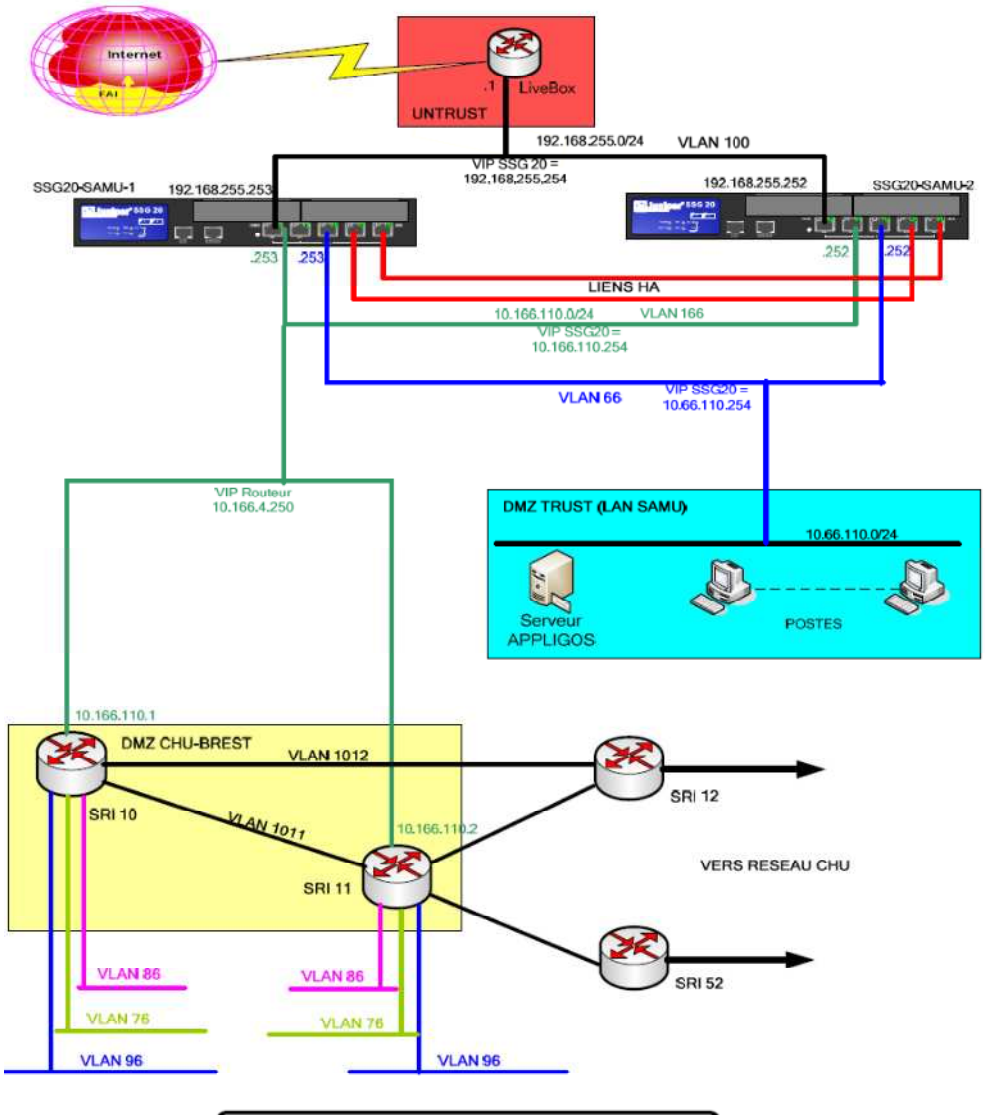


4.2.8.4 CONTINUITES RESEAU INFORMATIQUE / INTERNET

L'équipe réseau du CHRU de Brest a imaginé une architecture réseau répondant à 3 scénarii de sinistres :

- Pertes d'un élément réseau,
- Attaque virale,
- Défaillance éventuelle du FAI du CHRU, à savoir SFR.

La mise place des firewalls et la configuration de Vlan spécifique au SAMU, va permettre à la survenance d'une attaque virale d'isoler complètement l'architecture du SAMU. Le réseau devient indépendant du reste du réseau CHRU. La live-box permet un accès à internet en mode dégradé. La redondance des éléments réseaux permet de se prémunir d'une perte d'un élément actif réseau. Enfin les Vlan permettent de mettre à disposition des prestataires l'accès aux serveurs dont ils ont la charge en terme de maintenance, et cela d'une manière sécurisée. L'achat des 2 firewalls est réalisé, l'installation de ceux ci est planifiée pour septembre.



Figue 34 – Architecture réseau du Samu 29

4.2.8.5 PROTECTION DES DONNEES

La gestion des dossiers patients est assurée par la solution Applisamu de la société Appligos. Une architecture San a été mise en œuvre, elle permet la réplication synchrone des données du serveur principal Appligos, vers le site de secours.

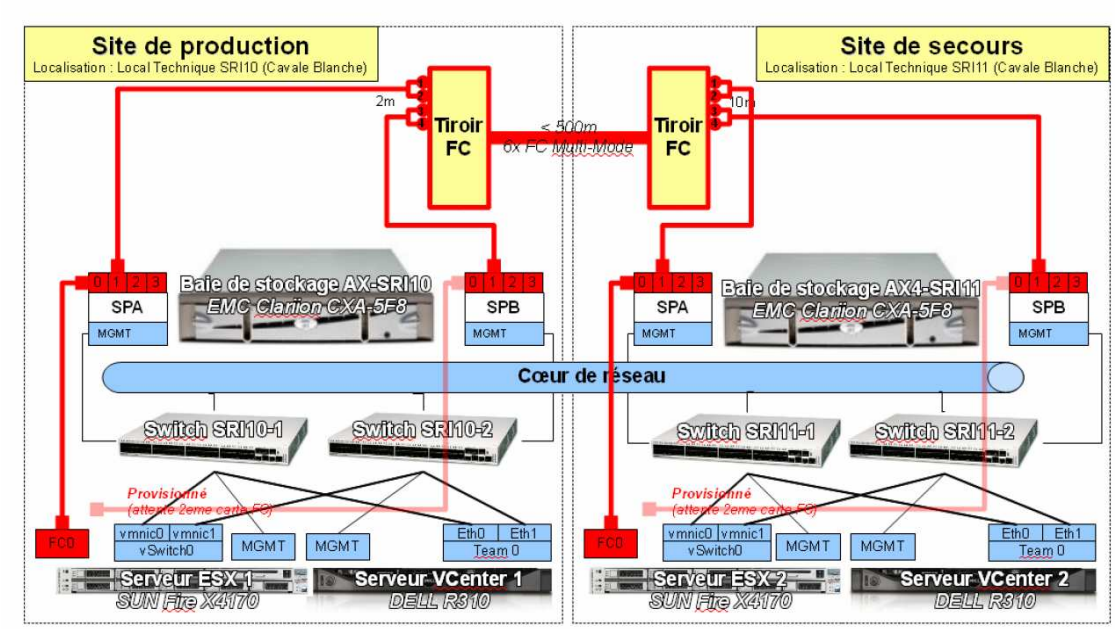


Figure 35 – Architecture SAN du Samu 29

La solution Applisamu se compose d'un serveur virtuel applicatif samu29-inter, et d'un serveur virtuel de base de données samu29-oracle.

Le système « Site recovery » vSphere de Vmware permet une relance des machines virtuelles sur le site de secours.

Les sauvegardes des bases de données et fichiers critiques sont réalisées en local sur le site de secours. Ces bases de données et fichiers sont en plus sauvegardés tous les jours par la DSIS.

4.2.8.6 RECAPITULATIF DETAILLE DE L'ARCHITECTURE

Nom Serveurs	Machine Physique	Fonctions	Acteurs principales
srv-samu-gen01	SRV15-1	Serveur Principale Genesys	Nextiraone
srv-samu-genbdd	SRV15-1	Serveur BDD Genesys	
srv-samu-wbm	SRV15-1	Serveur Soft Panel	
srv-samu-4760	SRV15-1	Serveur d'administration OXE	
srv-samu-mobi	SRV-SAMU-MOBI	Serveur d'appel Mobical	
srv-samu-snmp	SRV15-1	Serveur d'alerte snmp	
OXE 1	OXE 1	Autocommutateur 1	Service technique
OXO	OXO	Autocommutateur de secours	Service technique
Assmann 1	Assman 1	Enregistreur Assman 1	Assman
srv-samu-gen02	SRV16-1	Serveur secondaire Genesys	Nextiraone
OXE 2	OXE 2	Autocommutateur 2	Service technique
Assman 2	Assman 2	Enregistreur Assman 2	Assman
samu29-esx1	ESX1	Serveur Principal Applisamu	Appligos
samu29-esx2	ESX2	Serveur de secours Applisamu	Appligos
samu29-oracle	ESX1/ESX2	Serveur de base de données appligos	Appligos
samu29-inter	ESX1/ESX2	Serveur applicatif Appligos	Appligos
SRV15-1	SRV15-1	Serveur Physique	DSIS
SRV16-1	SRV16-1	Serveur Physique	DSIS

Tableau 5 – Tableau des éléments d'architecture Samu

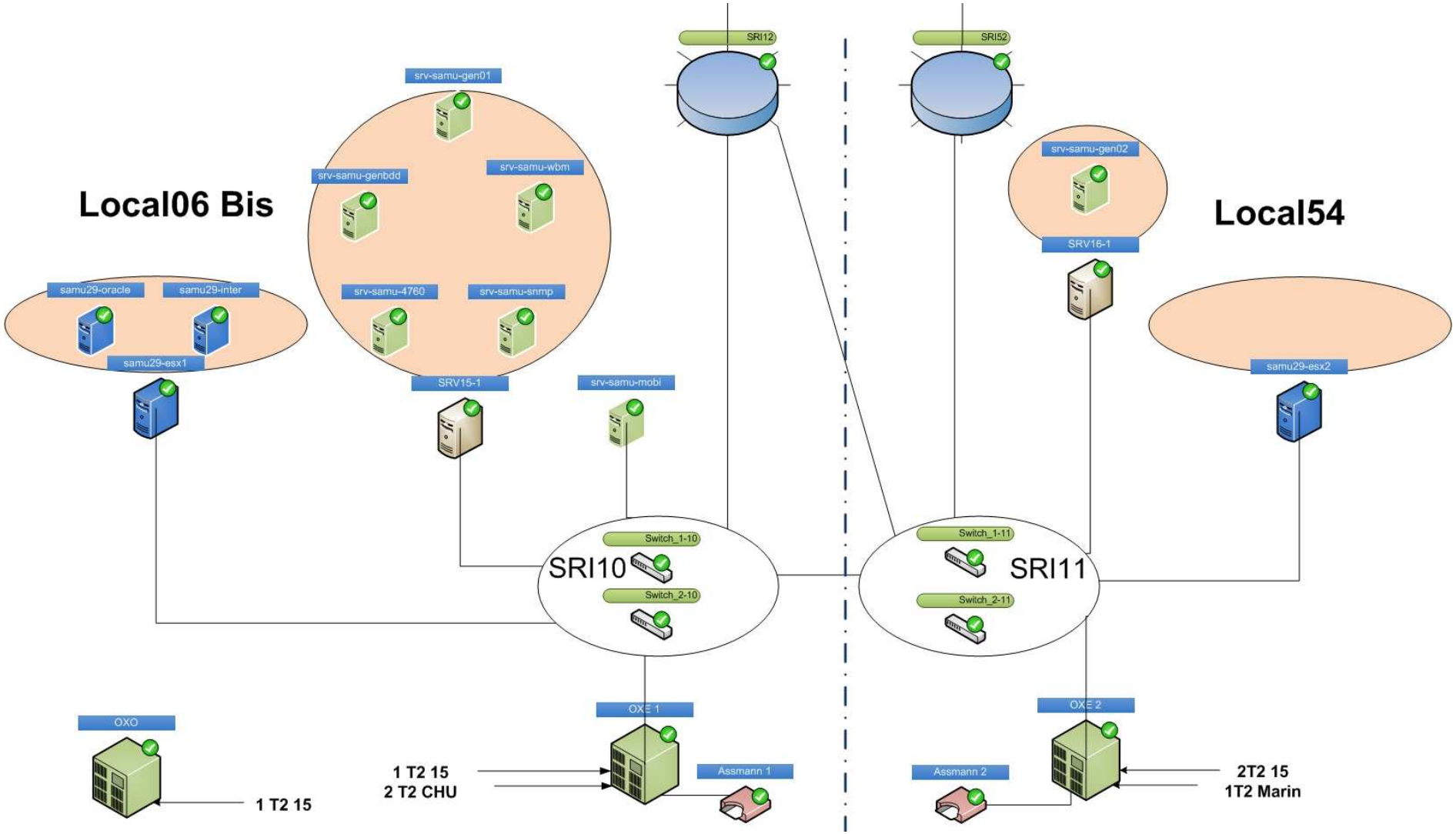


Figure 32 – schéma d'architecture Samu 29

4.2.9 ELABORATION DES PLANS DE CONTINUITE

4.2.9.1 PLAN DE GESTION DE CRISE

Ce document décrit l'ensemble des acteurs et leurs responsabilités.

Il comprend le synoptique de la gestion de crise, de la survenance du sinistre au retour fonctionnel et technique initial.

4.2.9.2 PLAN DE CONTINUITE ET DE REPRISE INFORMATIQUE

Ce document décrit l'architecture informatique lié au SAMU, il décrit également les mesures techniques de secours mises en œuvre pour assurer la continuité informatique des applications métiers.

Ce plan contient en annexe, les fiches réflexes informatiques DSIS, et dossiers techniques Nextiraone, Appligos.

4.2.9.3 PLAN DE CONTINUITE ET DE REPRISE TELEPHONIQUE

Ce document décrit l'architecture téléphonie du CHRU et spécifiquement du SAMU, il décrit également les mesures techniques de secours mises en œuvre pour assurer la continuité téléphonique.

Ce plan contient en annexe, les fiches réflexes techniques liées à la téléphonie des services techniques, et les dossiers techniques Nextiraone.

4.1.9.4 PLAN DE SAUVEGARDE

Ce document décrit les processus de sauvegarde mis en œuvre pour assurer les sauvegardes des données liées au SAMU. Il contient également les procédures de restauration de chaque type de données sauvegardées.

4.2.9.5 PLAN DE TEST

Ce document contient le descriptif des recettes effectuées lors de la VA (Vérification d'Aptitude) et de la VSR (Vérification de Service Régulier). Un planning des tests effectués est tenu à jour. Les scénarii de tests et les rapports de ceux-ci sont ajoutés en annexe.

4.2.9.6 PLAN DE CONTINUITE ET DE REPRISE FONCTIONNELLE

Ce document décrit les mesures à mettre en œuvre à la survenance d'une panne, quelle que soit l'origine. En annexe de ce document, on retrouvera les procédures dégradées utilisateurs.

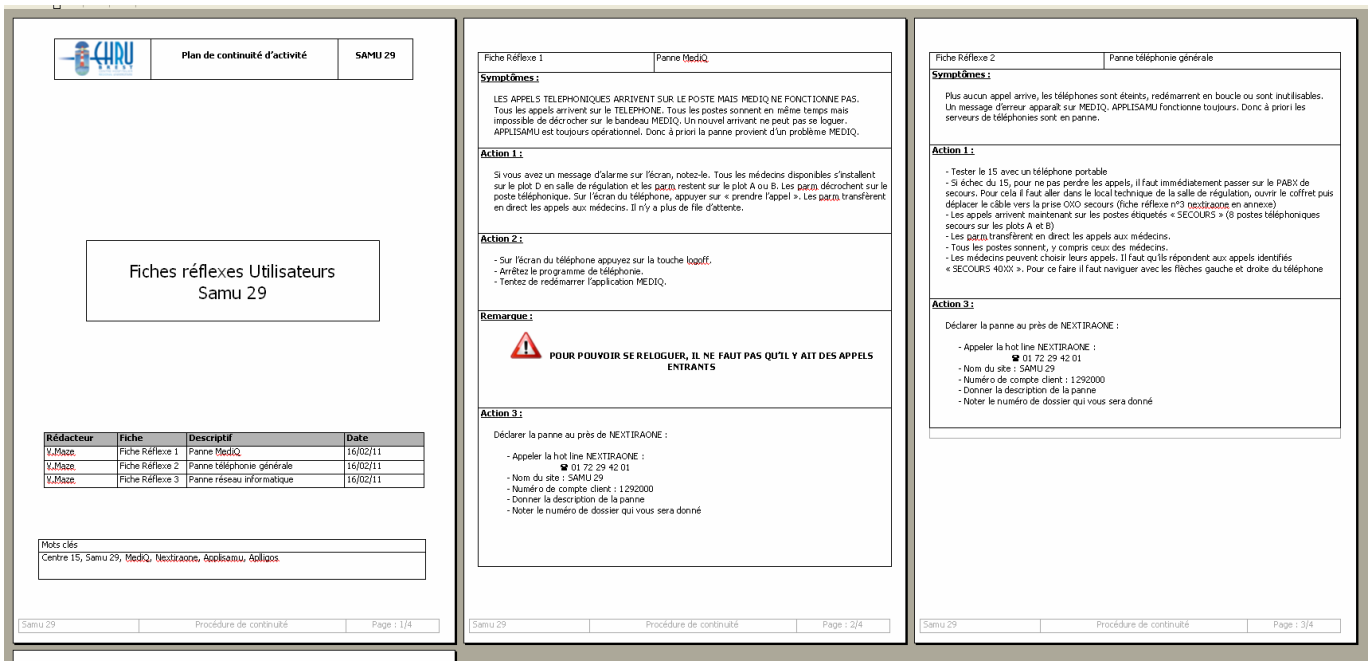


Figure 36 – Extrait de la procédure dégradée Samu 29

4.2.10 TEST DE CONTINUITE DE SERVICE

Un test de continuité de service est planifié le 28 juin 2011

Le scénario de panne retenu pour le test est la perte complète des éléments composant le SRI10 se trouvant dans le local 06 Bis.

5. BILAN PERSONNEL ET PERSPECTIVES

Ce projet de mémoire se déroule au sein de la DSIS et s'est réalisé avec la plupart des membres qui composent ce service. La disponibilité, le professionnalisme de ces personnes sont formidables. Je prends un réel plaisir à évoluer dans ce service et m'astreins à le rendre au mieux.

Le PCRI est prévu d'être opérationnel pour fin 2012. L'organisation du projet et les analyses propres au PCRI sont pleinement effectuées. Les phases de rédaction des plans de continuité et une partie des opérations mises en avant dans le plan d'action sont en cours.

Lors de mes quatre années en tant qu'administrateur San et systèmes Unix et pour avoir travaillé en étroite collaboration avec les autres membres du groupe technologies (réseaux, DBA, équipe micro) sur des projets communs, j'ai acquis une connaissance générale des éléments techniques de l'infrastructure informatique du CHRU. Ce projet du mémoire m'a permis de compléter mes connaissances dans la cartographie applicative du SI de l'hôpital et d'avoir une vision transversale couvrant une large partie du SI.

Les membres de l'équipe de pilotage m'ont aidé à recadrer et prioriser mes tâches projets. En effet, de par leur expérience à mener à bien les projets, ils m'ont tout au long des ces 10 derniers mois conseillé et accompagné.

Le projet PCA local SAMU m'a permis de modifier ma vision de la place du SI dans l'hôpital. En effet je me suis rendu compte que je devais cesser de voir l'hôpital au travers le prisme du Système d'Information, et que je devais replacer le soin et les patients au centre des réflexions.

En traitant ces projets, j'ai été amené à conduire des réunions et à gérer les désaccords et les différences d'opinion, à travailler en collaboration directe avec des personnes de différents métiers : directeurs, cadres de soin, informaticiens, médecins, infirmiers, permanenciers …. Cela est pour moi une formidable expérience.

Je pense que la mise en œuvre du PCA local SAMU, a contribué à faire reconnaitre le savoir faire de la DSIS dans le service du SAMU.

La réussite de ce projet va me permettre de présenter un cas concret et de m'appuyer sur une méthode éprouvée lors de déploiement de PCA à d'autres services de l'hôpital.

Enfin, ce projet de mémoire m'a permis de me conforter dans l'idée que j'ai du métier d'ingénieur et plus spécifiquement de celui de responsable sécurité du système d'information.

6. BIBLIOGRAPHIE

Articles et ouvrages

« Plan de continuité d'activité et système d'information vers l'entreprise résiliente », de Matthieu Bennasar

Magazine 01 Informatique

Sites Internet

http://www.zdnet.fr/actualites/plan-de-continuite-d-activite-quelle-demarche-adopter-39191691.htm

http://www.ssi-conseil.com/downloads/Methodologie-PCA-v1.1.pdf (CLUSIR)

http://itil.fr/DRP/PCA/drppca-mettre-en-oeuvre-un-plan-de-continuite-dactivite.html

http://www.hsc.fr/presse/clubpca/LIVRE-BLANC-CCA.pdf

http://www.sham.fr/

http://www.ssi-conseil.com/content/view/103/132/

http://www.ssi.gouv.fr/site_article45.html

http://www.clusif.asso.fr/fr/production/mehari/mehari.asp

http://www.27000.org/iso-27002.htm

http://www.gmsih.eu/fre/nos_activites/standards_et_interoperabilite/objectifs

https://www.uniha.org/

http://www.altairconseil.fr/plan-de-continuite.html

http://www.reseaux-telecoms.net/actualites/lire-virtualisation-et-consolidation-pour-le-pra-de-la-mutuelle-agpm-17961-page-3.html

http://www.duquesnegroup.com/PCA-Analyse-des-risques-et-Bilan-d-Impact_a97.html

7. GLOSSAIRE

CHRU : Centre Hospitalier Régional Universitaire

DSIS : Direction du Système d'Information de Santé

SI : Système d'information

GCS : Groupement de Coopération Sanitaire

ARS : Agence Régionale de Santé

EBIOS : Expression des besoins et indentification des objectifs de sécurité.

Mehari : aides intégrées pour l'évaluation des risques et la sélection des plans de sécurité

iso27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information

GMSIH : Groupement pour la modernisation des systèmes d'information hospitalier

UNIHA : Achat groupé des CHU de France

SPOF (Single Point Of Failure) : Élément non redondé qui représente un risque pour l'organisme ou le système.

IAE : L'Intégration d'applications d'entreprise ou IAE (en anglais Enterprise Application Intégration, EAI) est une architecture inter-logicielle permettant à des applications hétérogènes de gérer leurs échanges.