TD Sécurité

Plan de Reprise d'Activité

2018

Ce TD est dans la continuité du TD précédent concernant la PSSI.

Le but est de vous faire découvrir ce qu'est un PRA.

A partir du canevas de PRA ci-joint vous allez décrire les grandes lignes du plan de reprise d'activité de la société « Direct Petits Fours ».

Là encore, il n'est matériellement pas possible de réaliser un tel document dans le temps d'un TD.

Vous allez donc le compléter en vous concentrant prioritairement sur les chapitres : 3 et 5.

PLAN DE REPRISE D'ACTIVITÉ DU SYSTÈME D'INFORMATION

SOMMAIRE

GLOSSAIRE

LIBELLÉ	DÉFINITION
E.RS.I.	**Entité responsable du système d'information :** en général le service informatique ou la Direction du Système d'Information
E.S.	**Etablissement de Santé**
G.T.C.	**GESTION TECHNIQUE CENTRALISÉE :** dispositif de remontée d'alertes ou de données techniques
P.T.I.	**Protection des travailleurs isolés :** système d'alerte

1. Définitions et périmètres

1.1 Définition du P.R.A.

Le Plan de Reprise d'Activité [PRA] est le document qui décrit l'ensemble des dispositions et recense les procédures pour la reprise des applications et des données critiques suite à un sinistre informatique et la mise en œuvre d'un éventuel mode dégradé des applications.

Le PRA indique également selon quelles modalités les utilisateurs sont informés, du début à la fin du sinistre.

1.2 Objectifs

Le présent document a pour objectif de décrire le Plan de Reprise d'Activité (PRA) du système d'information de *[Indiquer le nom de l'établissement de santé]*. Le document liste le minimum de dispositions que doit prévoir l'établissement pour assurer la reprise de l'activité de son système d'information en cas de crise majeure ou importante du centre informatique.

Ce document présente les questions que l'établissement de santé s'est posées relativement aux points suivants :

- **Quelles sont les applications « métier » exploitées par l'établissement de santé** ?
- **Quel plan de sauvegarde des données contenues dans le système d'information l'établissement a-t-il élaboré ?**
- **Quelles sont les modalités de redémarrage du système d'information en cas de panne** ;
- **Comment les utilisateurs sont ils informés ?**
- **Comment s'articule le présent PRA avec le plan de continuité d'activité [PCA]**[1] **;**

1.3 Cellule de crise

L'établissement a créé une Cellule de Crise spécifique pour les dysfonctionnements graves du système d'information.

GUIDE Voir le guide d'élaboration pour sa composition

La cellule doit à la fois
- prendre des décisions liées à la reprise d'activité, lorsque plusieurs alternatives sont proposées par l'E.R.S.I.,
- coordonner la communication de crise envers les utilisateurs,
- coordonner les actions internes à l'établissement lorsque plusieurs professions sont impliquées dans le dysfonctionnement.

1.4 Périmètre du P.R.A.

[1] Le PCA décrit en particulier la conduite à tenir par les utilisateurs du système d'information en cas de panne informatique.

L'activité couverte par le présent plan de reprise concerne en premier lieu l'ensemble des composantes du système d'information de l'établissement. Comme il est présenté dans les paragraphes suivants, ces composantes sont :

- Les logiciels utilisés par les professionnels,
- Les flux de communication (échanges de données) entre les logiciels,
- Les machines (serveurs, postes de travail…) sur lesquels fonctionnent ces logiciels,
- Le réseau informatique qui permet la communication entre ces machines.
- Les dispositifs de sauvegarde des données.

Voir le guide d'élaboration pour vous aider à déterminer si le périmètre du P.R.A. doit être élargi aux éléments communicant via le réseau informatique mais ne faisant pas partie du système d'information, et/ou à la téléphonie.

1.5 Philosophie de construction du P.R.A.

Conformément à la démarche de la D.G.O.S., le présent P.R.A. a été construit avec l'objectif général **d'anticiper les questions qui vont se poser au moment d'un sinistre majeur**, et d'avoir prévu les éléments nécessaires à une reprise à la fois rapide et sure.

Pour cela, la **première étape** consiste à **inventorier les applications informatiques**, et à en évaluer la criticité, en lien avec les **besoins en disponibilité** exprimés par leurs utilisateurs.

Dans un **second temps**, le P.R.A. fait le **lien entre les applications informatiques et le matériel** sur lequel elles sont installées, ce qui permet de réaliser l'inventaire de ce matériel.

La **troisième étape** décrit les **modalités de sauvegarde et de restauration des données**, que l'E.R.S.I. pourrait être amené à utiliser dans le cadre du redémarrage du système.

Le **quatrième point** aborde **l'éventualité de continuer à utiliser certains logiciels « en mode dégradé »** pendant le sinistre.

Le **cinquième paragraphe** dresse la liste des actions à mener pour **diagnostiquer l'origine du sinistre**, **évaluer ses conséquences** en particulier la **durée d'indisponibilité.**

Le dernier élément recense les **éléments du socle technique**, hors les serveurs sur lesquels sont installés les logiciels, qui sont **indispensables au redémarrage** du système d'information.

L'ensemble de ces étapes permet de déterminer un **ordre préférentiel de redémarrage**.

2. Infrastructure fonctionnelle et inventaire des biens

Se reporter au répertoire « Inventaire des biens » dans lequel un classeur de description des infrastructures techniques et applicatives ainsi qu'un exemple de cartographie sont disponibles pour formaliser l'inventaire nécessaire au PRA.

Ces outils permettent avant tout, sur la base des besoins en disponibilité, de définir un ordre de priorité dans le redémarrage des applications. Pour affiner les priorités de démarrage, il convient de prendre en compte les interactions et dépendances entre applications, dont les flux sont décrits dans l'onglet « Tableau des interfaces » du classeur « Inventaire des biens ».

3. Dispositions prévues pour la récupération des données

3.1 Organisation et matériel pour la sauvegarde des données

La sauvegarde des données contenues dans le système d'information de l'établissement est placée sous la responsabilité de *[nom de l'établissement / nom des sociétés en charge de la maintenance du système d'information ou nom de la personne de l'établissement].*

Les dispositifs de sauvegarde des données détenus par l'établissement sont ici décrits :

– *[Présenter ici les dispositifs de sauvegarde dont dispose l'établissement de santé (exemples : boitier de sauvegarde, robot, …)] ;*

GUIDE Voir le guide d'élaboration pour déterminer les informations à faire figurer dans ce document, si le plan de Sauvegarde est déjà formalisé ou pas.

3.2 Questions posées sur la récupération des données

Chaque cas occasionnant l'utilisation du PRA étant particulier concernant la récupération des données et la restauration des sauvegardes, il n'est pas possible d'établir des procédures de récupération des données *a priori.*

Dans le contexte d'un PRA, il est plus pertinent de se poser les questions clés suivantes, qui détermineront la conduite à tenir :

- Quelle est la dernière situation stable du système d'information ?
  - Est-il possible de revenir à cette situation ?
  - Si oui, faut-il avoir recours à une sauvegarde ou pas ?
- Diagnostic de la perte de données :
  - Y a-t'il un risque que des données aient été perdues ?
  - Si oui, est-il possible de déterminer dans un délai et avec des moyens raisonnables la nature et le volume des données perdues, l'ampleur et la gravité de la perte ?
- Quelles sont les sauvegardes disponibles ?
- Quels sont les liens entre logiciels ?
  - Y-a-t'il un risque de désynchronisation entre les différentes applications ?
  - Si oui, mesurer si d'autres restaurations de données sont nécessaires.
- Détermination des données récupérables en fonction des données perdues et des sauvegardes disponibles
- Délai de réalisation : une évaluation du délai pour récupérer les données nécessaires doit être effectuée.
- Décision : Tous les éléments sont-ils réunis et présentables pour permettre une décision de restauration de données ?

Ces éléments sont présentés à *[indiquer l'instance décisionnaire de l'établissement]* qui décide, sur la base de ces éléments, de la conduite de l'E.R.S.I. vis à vis des données éventuelles à récupérer.

GUIDE Voir le guide d'élaboration pour les recommandations sur la responsabilité de la prise de décision de restaurer une sauvegarde (donc de perdre des données)

3.3 Plan de sauvegarde des données

Le plan de sauvegarde des données présente pour chaque logiciel les 3 items permettant de juger de la pertinence des données sauvegardées :

- **Le type** : Total et/ou incrémental (qui ne sauvegarde que les différences d'une fois sur l'autre
- **La fréquence** de sauvegarde pour chaque type
- **La période de rétention des données,** c'est à dire la durée de conservation d'une sauvegarde.

Le plan indique également où sont physiquement conservées ces sauvegardes et sur quels supports, ainsi que la nature des tests de restauration effectués.

La politique de sauvegarde de données est décrite dans la Politique de Sécurité du Système d'Information. Elle porte sur les règles de sauvegarde, de vérification et de tests de restauration. Dans le cadre du PRA, le plan de sauvegarde décrit les modalités de sauvegarde, de contrôle, de tests de restauration précisément. Un exemple de « Plan de sauvegarde »[2] et un exemple « Procédure de gestion des bandes de sauvegarde » sont disponibles dans le répertoire PRA.

3.4 Mode de mise en œuvre de la récupération des données

Suivant la décision prise, l'ordre de restauration sera déterminé en se référant aux tableaux du fichier d'inventaire.

Les référents métiers (identifiés au préalable) devront pouvoir vérifier la bonne récupération des données prévues.

[indiquer toute information facilitant l'implication des référents métiers]

3.5 Bilan de la récupération des données

Il devra ensuite être évalué quelles données ont été perdues, et le stade de redémarrage effectif.
[indiquer le mode de communication de ces informations aux utilisateurs]

[2] L'exemple proposé n'intègre pas les contrôles et les procédures de tests.

4. Dispositions prévues pour le fonctionnement des applications en mode dégradé et le retour à la normale

GUIDE Voir le guide pour adapter ce paragraphe à votre contexte

[indiquer l'instance décisionnaire de l'établissement] peut selon le cas décider d'un fonctionnement des applications en mode dégradé.

Cette disposition est à bien différencier du Plan de Continuité d'Activité [PCA], qui consiste à décider d'un fonctionnement de l'hôpital ou de l'un de ses processus sans informatique. Ici, il s'agit bien d'un fonctionnement dégradé de l'informatique,

- soit en termes de performances (remplacement d'un serveur défectueux par une machine moins puissante ou un PC)
- soit en termes de communication (non fonctionnement des interfaces)
- soit en termes de données (pas d'historique, pas de nouveau patient, disponibilité partielle des données…)

Chaque cas étant particulier, il n'est là non plus pas possible de déterminer a priori une conduite à tenir. Il conviendra néanmoins d'avoir une véritable réflexion bénéfices / risques en la matière, le fonctionnement en mode dégradé pouvant être source de perturbations importantes bien après la sortie de crise.

5. Dispositions prévues pour le redémarrage des applications

5.1 Diagnostic du dysfonctionnement

L'E.R.S.I. pose le diagnostic en évaluant successivement les causes possibles du dysfonctionnement, qui sont décrites ici dans l'ordre à étudier :

- Alimentation électrique et onduleur(s) *[indiquer ici qui gère le problème électrique dans son ensemble, du diagnostic électrique au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires, références d'un éventuel contrat de maintenance]*

- Climatisation *[indiquer ici qui gère le problème de climatisation dans son ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

- Dégât des eaux *[indiquer ici qui gère le problème dans son ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

- Sécurité incendie *[indiquer ici qui gère le problème de sécurité incendie dans son ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

- Réseau et transport de données externes *[indiquer ici qui gère le réseau et transport de données externes dans son ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

- Réseau local (éléments actifs, routeurs, pare-feux…) *[indiquer ici qui gère le réseau local dans son ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

- Machines de stockage centralisé (SAN, NAS et éléments actifs associés) *[indiquer ici qui gère les machines de stockage centralisé dans leur ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

- Serveurs physiques (alimentation électrique interne, cartes réseau, disques durs…) *[indiquer ici qui gère les serveurs physiques dans leur ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

- Serveurs d'accès au système d'information (alimentation électrique interne, cartes réseau, disques durs…) *[indiquer ici qui gère les serveurs physiques dans leur ensemble, du diagnostic au contact avec d'éventuels intervenants extérieurs jusqu'à la validation du retour à la normale : coordonnées du responsable suivant les plages horaires]*

5.2 Conséquences du dysfonctionnement et pré-requis au démarrage

L'E.R.S.I. évalue les conséquences de la panne, pour déterminer s'il peut redémarrer le système d'information dans un état normal complet, ou dans un mode dégradé.

Il détermine ensuite

- **si l'intégrité des données a été touchée** (ou estime le risque qu'elle l'ait été), et présente toutes les alternatives possibles à la Cellule de Crise.
- Le **délai de rétablissement d'un fonctionnement** (normal ou dégradé) qui doit être estimée en tenant compte selon les cas :
  - des modalités d'intervention des prestataires extérieurs (couverture heures ouvrées ou 24/7)
  - de la durée de rétablissement de l'environnement (électricité, sécurité) permettant le fonctionnement de l'architecture
  - de la durée de réparation matérielle ou logicielle
  - de la durée de restauration des données
  - de la durée de redémarrage du système, tests compris.

Dans le cas d'un passage en fonctionnement dégradé, il convient d'évaluer selon le même principe le délai de retour à la normale.

5.3 Socle commun technique du systeme

5.3.1 Description du socle commun

La description détaillée du socle technique commun figure au paragraphe 7.1

5.3.2 Ordre de redémarrage du socle commun

Une fois que les référents techniques ont vérifié que la situation est compatible avec un redémarrage, il convient de respecter un ordre de remise en fonction lié aux contraintes techniques propres à chaque système d'information.

L'ordre de redémarrage est décliné dans l'onglet « Socle Commun » du fichier « Inventaire des biens » :

GUIDE Voir le guide d'élaboration pour la « check list » dans les cas les plus courants.

5.4. Redémarrage des applications en mode dégradé

La cellule de crise devra statuer sur un redémarrage en mode dégradé, qui pourrait être, selon les possibilités proposées par les différents logiciels et la cohérence du système :

- un redémarrage d'un ou plusieurs logiciels en mode « secours » ou « lecture seule »
- un redémarrage d'un ou plusieurs logiciels indépendamment du fonctionnement de certaines interfaces avec lesquelles il(s) communique(ent).
- Un redémarrage d'un ou plusieurs logiciels considéré(s) comme indispensable(s), sans pour autant redémarrer l'ensemble du système.

5.5 Ordre de redémarrage des applications

L'ordre de redémarrage **théorique** des applications est déduit du tableau général figurant dans l'onglet « Liens Fonctionnalité – Logiciel » du fichier « Inventaire des biens », et figure dans l'onglet « Ordre de redémarrage théorique » du même fichier.

5.6 Plan de redémarrage des applications

Tous les éléments sont réunis pour que **la cellule de crise valide le plan de redémarrage des applications**, adaptée à la situation de crise en cours.

L'ordre de redémarrage réel est décrit dans l'onglet « Plan de redémarrage » du fichier Excel. C'est la feuille de route que les informaticiens doivent suivre jusqu'à la résolution définitive de la crise.

GUIDE Voir le guide d'élaboration pour l'explication de la manière dont cet onglet est conçu, en reprenant l'ensemble des informations pertinentes du PRA : socle commun, priorités serveurs induites par criticité logiciels, mode dégradé, reprise de données.

Pour valider ce plan, la cellule de crise doit :

- Avoir statué, après explications de l'E.R.S.I., sur les variations entre le plan théorique et la situation réelle
- Avoir décidé d'un redémarrage total ou en mode dégradé, en prenant en compte les coûts (remplacement de matériel ou recours à un prestataire extérieur par exemple), les délais et les impacts pour les activités métiers.
- Avoir décidé d'une reprise ou non de données (induisant éventuellement une perte de données)

Le choix de la cellule de crise est validé et formalisé.

GUIDE Voir le guide d'élaboration pour des exemples sur ces 3 points

6. Information des utilisateurs en cas de panne

6.1 Nature des informations transmises

Les utilisateurs sont informés par la cellule de crise
- du choix du scénario de redémarrage retenu,
- de la décision de procéder à une restauration des données,
- des conséquences que cela va entraîner,
- de la durée estimée de l'opération, et, le cas échéant, des perturbations ou des indisponibilités générées par l'opération

6.2 Modalites de diffusion de l'information

L'établissement doit définir ici la manière dont l'information sera diffusée, en prévoyant bien entendu une alternative à la messagerie informatisée, voire aux communications téléphoniques.

7. INFORMATIONS TECHNIQUES ET POINTS DE VIGILANCE

La reprise d'activité ne peut s'envisager qu'à la condition que l'infrastructure technique sur laquelle repose l'ensemble des activités informatisées soit opérationnelle.
Pour s'en assurer, ce paragraphe va décrire cette infrastructure, à la fois d'un point de vue architectural, et de localisation géographique.
L'environnement sécurisant cet ensemble sera également décrit (sécurité incendie, alimentation électrique, climatisation, protections contre les dégâts des eaux…).

Pour compléter le PRA du système d'information, l'établissement de santé pourra notamment intégrer des informations relatives :

- A l'infrastructure technique de l'établissement de santé : cartographie de l'infrastructure technique, lieu géographique de l'infrastructure, description de la salle informatique, du centre d'hébergement, … ;
- Aux principes de sécurité qu'il aura définis pour garantir la continuité d'activité et le retour à la normale du système d'information en cas de panne : sécurité des serveurs, supervision et contrôle, protection logicielle, stockage, …

7.1 INFRASTRUCTURE TECHNIQUE

7.1.1 Présentation de l'architecture technique

Cette section décrit les ressources techniques de l'établissement de santé. La cartographie technique du système d'information pourra ainsi être ici intégrée.

Pourront également être précisées des informations relatives à la liste des serveurs exploités : serveur de données, d'application, serveurs disponibles par environnement, …

GUIDE Voir le guide d'élaboration pour des exemples de schéma d'architecture technique

7.1.2 Lieu géographique

Cette section présente la localisation géographique de l'infrastructure technique de l'établissement de santé, selon que celle-ci soit hébergée sur un site unique, ou réparti sur des lieux géographiques distincts.

Il convient donc de ne conserver ici que le paragraphe correspondant à la situation de l'établissement de santé, puis de le renseigner des informations indiquées.

- Votre établissement a confié l'hébergement de son système d'information à un tiers :

L'infrastructure technique du ***[nom de l'établissement de santé]*** est hébergée par ***[nom de la société en charge de l'hébergement de l'infrastructure technique de l'établissement]***.

Elle est ***[localisée sur un seul site géographique / réparti(e) sur plusieurs sites comme suit :***

- ***Localisation géographie de la salle informatique ;***
- ***Localisation géographique du centre d'hébergement (le site de production et le site de secours).***

– Votre établissement héberge le système d'information :

L'établissement de santé héberge lui-même l'infrastructure technique. Celle-ci est ***[localisée sur un seul site géographique / réparti(e) sur plusieurs sites géographiques comme suit :***

- ***Localisation géographique de la salle ou des salles informatique ;***

7.1.3 Description des locaux

Cette section présente les caractéristiques de sécurisation des locaux qui hébergent l'infrastructure technique de l'établissement de santé. Pour chaque local identifié, les informations suivantes sont notamment précisées :

- La sécurisation de l'accès aux locaux ;
- L'alimentation électrique ;
- La climatisation ;
- La sécurité en cas de dégâts des eaux ;
- La détection d'incendie.

L'établissement de santé ajoutera ici toute information sur les caractéristiques de sécurisation des locaux hébergeant l'infrastructure technique qu'il juge pertinent d'intégrer au présent PRA.

De plus, il ajoutera en tant que de besoin les autres locaux qui n'hébergent pas l'infrastructure technique de l'établissement mais qui pourraient avoir un impact sur le fonctionnement des équipements de l'infrastructure technique (ex : salle de l'auto commutateur).

Les caractéristiques générales de sécurisation de la salle informatique sont présentées ci-après.

La sécurisation de l'accès à la salle informatique

Les informations suivantes sur la sécurisation de l'accès à la salle informatique seront notamment indiquées :

- La localisation de la salle informatique (site géographique, emplacement au sein de l'établissement, …) ;
- Le mode de sécurisation de l'accès à la salle informatique (porte blindée, digicode, alarme, caméra de surveillance, contrôle des mouvements, …)

L'alimentation électrique

Les informations suivantes sur le système d'alimentation électrique seront notamment indiquées :

- La présence d'onduleurs permettant d'assurer le fonctionnement du système en cas de coupures ;
- La présence de groupes électrogènes de secours en cas de coupures d'électricité ;
- Les modalités de remontée d'alertes en cas de coupures d'électricité ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

Le bureau (la personne) responsable de la maintenance du système d'alimentation électrique

- Les dispositions du contrat de maintenance du système.

La climatisation

Les informations suivantes sur le système de climatisation seront notamment indiquées :

- La puissance du système de climatisation ;
- La température à laquelle est gardée la salle informatique ;
- Les modalités de remontée d'alertes en cas d'arrêt du système de climatisation ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

Le bureau (la personne) responsable de la maintenance du système de climatisation ;

- Les dispositions du contrat de maintenance du système de climatisation.

La sécurité en cas de dégâts des eaux

Les informations suivantes sur la sécurité mise en place en cas de dégâts des eaux seront notamment indiquées :

- Les modalités d'alerte en cas de présence d'eau (ex : système de détection, vase de rétention d'eau, …) ;
- L'équipement installé pour évacuer l'eau (ex : pompes de refoulement, …) ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système d'alertes et de l'équipement.

La détection d'incendie

Les informations suivantes sur le système de détection d'incendie seront notamment indiquées :

- L'équipement mis en place pour détecter / éteindre un incendie ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

Le bureau (la personne) responsable de la maintenance du système de détection d'incendie ;

- Les dispositions du contrat de maintenance du système de détection et d'extinction d'incendie.

7.1.4 Réseau et transport de données

Les informations suivantes sur le réseau de l'établissement de santé et les modalités de transport des données pourront notamment décrites :

- L'architecture du réseau (topologie du réseau local (LAN), WAN, protocoles de communication, bande passante, etc.) ;
- La description des services offerts par les opérateurs télécoms pour les échanges de l'établissement de santé avec l'extérieur (liaison spécifique/internet, bande passante garantie pour les échanges, engagements en cas de panne, etc.)

Synoptique général du réseau avec liens internes vers locaux techniques et lien externes.

7.2 Principes de sécurité

Cette section expose les principes de sécurité définis par l'établissement pour garantir la continuité d'activité et le retour à la normale du système d'information en cas de panne. Elle contient notamment les principes établis en matière de :

- Sécurité des serveurs ;
- Supervision et contrôles du système d'information ;
- Protection des logiciels ;
- Stockage.

L'établissement de santé pourra s'appuyer sur les termes des Contrats conclus avec les sociétés chargées de la maintenance du système d'information pour renseigner cette section.

Par ailleurs, l'établissement de santé ajoutera ici toute information sur les principes de sécurité qu'il juge pertinent d'intégrer au présent PRA.

7.2.1 Sécurité des serveurs

Indispensable

Les informations suivantes sur la sécurité des serveurs seront notamment indiquées :

- Le nombre et la description des serveurs (serveurs physiques / virtuels) ;
- Le cas échéant, la description de la plateforme gérant les serveurs virtuels ;
- La périodicité de réplication des serveurs du centre de production vers ceux du centre de secours ;
- Les modalités de reprise de l'activité d'un serveur en cas de panne ;
- La disponibilité des applications en cas de panne d'un serveur prévue par le Contrat conclu avec la société chargée de la maintenance du SI le cas échéant ;

- La procédure de bascule des serveurs et applications actifs du site de production vers le site de secours.

Facultatif

- En cas de panne du serveur, le délai contractuel de rétablissement conclu avec la société chargée de la maintenance.

7.2.2 Supervision et contrôle

Indispensable

Les informations suivantes sur les procédures de supervision et de contrôle du système d'information de l'établissement seront notamment indiquées :

- Les acteurs responsables de la surveillance du système (établissement, société de maintenance, ...) et leur plage horaire d'intervention.
- La description du système d'alertes mis en place en cas de dysfonctionnements (exemple : nagios) ;
- Les modalités de remontées de ces alertes auprès des acteurs concernés ;

Facultatif

…- l'éventuelle présence d'un système de contrôle des intrusions sur les serveurs ;

7.2.3 Protection du système

Indispensable

Une description sommaire des protections installées afin de protéger l'infrastructure technique de l'établissement seront indiquées :

- Protection des serveurs : mise à jour des OS,
- Protection des serveurs : protections contre les logiciels malveillants, … ;
- Protection des postes de travail : mise à jour des OS,
- Protection des postes de travail : protections contre les logiciels malveillants, … ;
- Protection de la messagerie : logiciel anti-spam,…
- Protection des accès extérieurs entrants ou sortants : filtrage URL
- Protection des accès extérieurs entrants ou sortants : pare-feu

7.2.4 Stockage

Cette section présente les principes de stockage des documents créés par les utilisateurs du système d'information de l'établissement de santé (« serveurs bureautique », clés USB,…)