Schéma directeur des espaces numériques de travail

Annexe Stratégie d'exploitation

Version 1.0

SOMMAIRE

1. Introduction ... 3

1.1 Contexte ... 3

1.2 Objectifs et contenu du document ... 4

1.3 Guide de lecture ... 4

1.4 Documents de référence et terminologie ... 5

2. Principes généraux ... 6

2.1 La qualité de service des ENT ... 6

2.2 L'atteinte des objectifs et les acteurs ... 6

2.3 Les prestataires et la contractualisation ... 8

2.3.1 Principes généraux ... 8
2.3.2 Relations entre intégrateur et mainteneur ... 9
2.3.3 Relations entre hébergeur/exploitant et intégrateur/mainteneur ... 9
2.3.4 Services standards et spécifiques ... 10
2.3.5 Propriété des matériels et logiciels ... 10
2.3.6 Qualités des prestataires extérieurs et exigences contractuelles ... 11

3. Les caractéristiques de l'ENT ... 12

3.1 Préambule ... 12

3.2 Dispositifs de sûreté de fonctionnement ... 12

3.2.1 Redondance des composants de l'ENT ... 12
3.2.2 Sécurisation des fluides ... 14

3.3 Surveillance, indicateurs, diagnostic et résolution de premier niveau ... 14

3.3.1 Surveillance ... 14
3.3.2 Outils d'analyse ... 15
3.3.3 Outils de mesure de la qualité de service ... 15

3.4 Autres outils d'exploitation ... 16

3.5 Gestion des configurations ... 16

3.6 Gestion des incidents ... 16

3.7 Dispositifs de sécurité ... 17

3.8 Plates-formes ... 17

4. Fourniture et évolutions de l'ENT ... 18

4.1 Fourniture initiale ... 18

4.2 Maintenance ... 19

4.2.1 Évolution dans le cadre d'une maintenance 19
4.2.2 Contractualisation 20
4.2.3 Gestion des changements 20

4.3 Les étapes préalables à une mise en exploitation 21

4.4 Livrables 22

4.5 Tests 23

4.6 Définition du planning de déploiement 24

4.7 Gestion de projet et des risques en phase de maintenance et d'exploitation 24

4.8 Audits 24

4.9 Réversibilité 24

5. Exploitation de l'ENT 25

5.1 Activités d'exploitation 25

5.2 Gestion des incidents et des problèmes 25
5.2.1 Définitions 26
5.2.2 Évaluation de la priorité d'un incident 26
5.2.3 Support 28
5.2.4 Traitement de l'incident 29
5.2.5 Reporting 30
5.2.6 Procédure d'escalade hiérarchique 31
5.2.7 Plan de Continuité de Service 31
5.2.8 Gestion de crise 31

5.3 L'exploitation courante 32
5.3.1 Journalisation 32
5.3.2 Sécurisation des données, sauvegarde et archivage 33
5.3.3 Lutte anti-virale 35
5.3.4 Gestion des droits et des flux 36

5.4 Mesures de la qualité de service 37
5.4.1 Disponibilité des services 37
5.4.2 Gestion et mesure des performances 38
5.4.3 Réactivité 39
5.4.4 Qualité du centre d'appel 40
5.4.5 Autres indicateurs 40

1. Introduction

1.1 Contexte

Le Schéma Directeur des Espaces numériques de Travail (SDET) [1] propose un ensemble de recommandations fonctionnelles, organisationnelles et techniques pour guider la mise en œuvre d'Espaces Numériques de Travail (ENT) dans les établissements d'enseignement.

En complément des grandes orientations proposées dans le document central du SDET, des thèmes sont traités de manière approfondie dans des annexes indépendantes :

- L'annexe « Recommandations pour l'Authentification–Autorisation–SSO : AAS » :

  Elle est consacrée à la sécurisation des accès aux services applicatifs proposés au travers des ENT.

- L'annexe Juridique :

  Elle apporte un éclairage sur les thèmes juridiques indispensables à la conduite d'un projet ENT.

- L'annexe « Stratégie d'exploitation » :

  Elle apporte des préconisations sur l'organisation de l'exploitation des ENT.

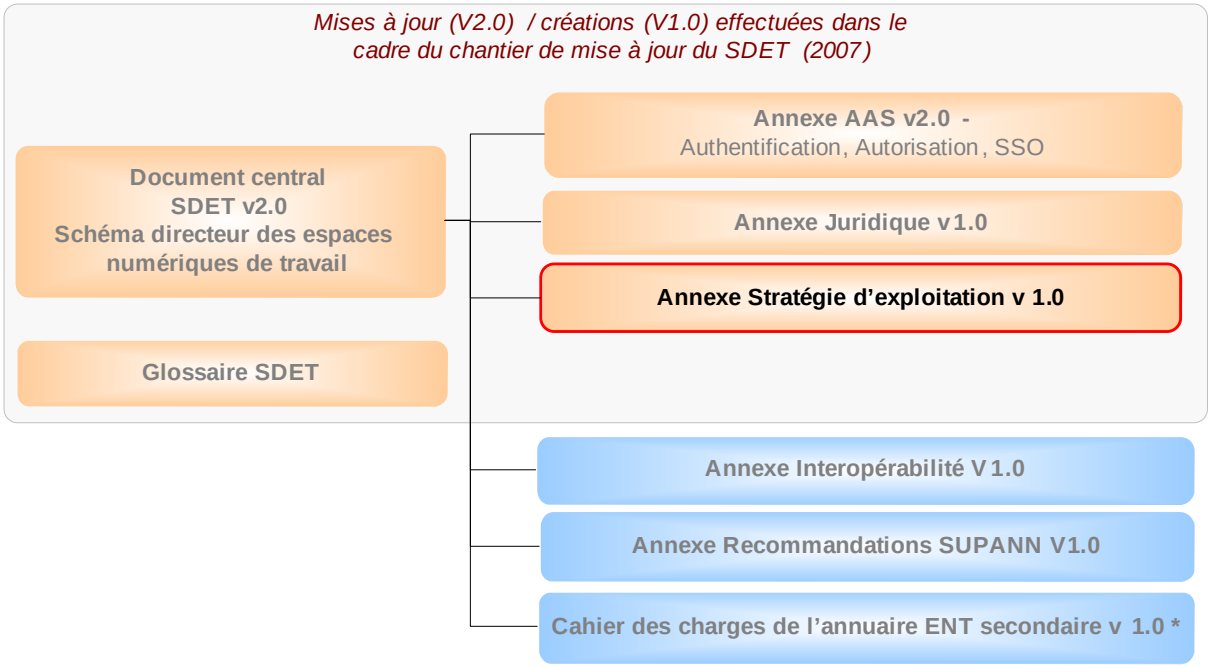
- L'annexe « Interopérabilité » [2] :

  Elle définit les standards à suivre et les conditions à respecter pour qu'un ENT soit interopérable avec les autres.

- L'annexe « Recommandations SUPANN » [3] :

  Elle émet des préconisations pour la compatibilité des annuaires de l'enseignement supérieur.

- Le cahier des charges de l'annuaire ENT secondaire



** Cette annexe est rédigée selon un format de cahier des charges générique que peuvent utiliser directement les porteurs de projet Les autres annexes sont rédigées selon un formalisme d'énoncé de règles et recommandations.*

Le présent document constitue l'annexe du schéma directeur des espaces numériques de travail (SDET) relatif à la stratégie d'exploitation.

1.2 Objectifs et contenu du document

Le niveau de qualité de service des ENT doit être élevé. Les horaires d'utilisation sont très étalés dans la journée et dans la semaine, au cours de l'année scolaire. Les pics de sollicitation des ressources peuvent être très importants et presque toujours prévisibles. Par ailleurs, les ENT contiennent des données sensibles et nécessitent, par conséquent, un niveau de sécurité élevé.

La garantie d'une qualité de service acceptable et pérenne, quelles que soient les évolutions de l'ENT, du contexte d'utilisation et de l'organisation interne et externe, exige la mise en place des moyens, des processus industriels et des contrats pour toutes les phases du projet, de la conception et réalisation, à la mise en exploitation et à la maintenance.

L'annexe Stratégie d'exploitation fournit donc un ensemble de recommandations pour la définition de l'architecture et pour les processus des différentes phases des projets qu'il faudra décliner pour l'ensemble des acteurs et intégrer dans la contractualisation de ces acteurs.

1.3 Guide de lecture

Niveaux de recommandation

Afin de déterminer le niveau d'obligation de respect des recommandations fournies dans ce document, la terminologie définie dans le RFC 2119 de l'IETF est utilisée, avec les traductions suivantes :

- MUST, SHALL : DOIT
- MUST NOT, SHALL NOT : NE DOIT PAS

- REQUIRED : EXIGÉ
- SHOULD : DEVRAIT
- SHOULD NOT : NE DEVRAIT PAS
- RECOMMENDED : RECOMMANDÉ
- MAY : PEUT
- OPTIONAL : FACULTATIF

La définition de ces termes issus du RFC 2119 et appliqués à ce document est la suivante :

- **DOIT** : ce mot, ou le terme « **EXIGÉ** », signifie que la définition est une exigence absolue de la spécification (i.e. du présent document).
- **NE DOIT PAS** : cette expression signifie que la définition est une interdiction absolue de la spécification (i.e. du présent document).
- **DEVRAIT** : ce mot, ou l'adjectif « **RECOMMANDÉ** », signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ne pas appliquer cette recommandation, mais les conséquences doivent être comprises et analysées soigneusement avant de choisir une autre option. Remarque : cette recommandation correspond à un conseil ou à une bonne pratique.
- **NE DEVRAIT PAS** : cette expression, ou l'expression « **NON RECOMMANDÉ** », signifie qu'il peut exister des raisons valables, dans des circonstances particulières, quand le comportement particulier est acceptable ou même utile, de suivre cette recommandation. Mais les conséquences doivent être comprises et le cas soigneusement pesé.
- **PEUT** : ce mot, ou l'adjectif « **FACULTATIF** », signifie qu'un item est vraiment facultatif. Un fournisseur peut inclure l'item parce qu'un marché particulier l'exige ou parce qu'il estime qu'il améliore le produit tandis qu'un autre fournisseur peut omettre le même item.

Nature des recommandations

Notons que les recommandations du document couvrent deux aspects :

- Certaines recommandations définissent des règles ou des principes à respecter.
- D'autres recommandations indiquent des travaux complémentaires à mener sur lesquels chaque acteur de projet ENT doit se positionner.

Enfin, afin d'étayer le propos, certaines recommandations sont illustrées par des cas d'usage, des retours d'expérience ou des précisions techniques.

1.4 Documents de référence et terminologie

Les documents de référence pour l'application des recommandations sont précisés à la fin de ce document (Appendice).

La terminologie utilisée dans ce document est définie dans le glossaire [7].

2. Principes généraux

2.1 La qualité de service des ENT

La qualité de service des ENT se caractérise notamment par :

- une disponibilité de l'ensemble des services offerts aux utilisateurs 24 heures sur 24, 365 jours par an. Il est toutefois possible de restreindre cette disponibilité pour certaines catégories d'usagers ou certains des services offerts ;
- des temps de réponse acceptables et l'accessibilité aux services y compris lors des périodes de forte activité ;
- la conservation de l'intégrité des données des utilisateurs et des contenus ;
- la sécurité et la confidentialité des données.

2.2 L'atteinte des objectifs et les acteurs

L'objectif de qualité de service doit être dicté dès le démarrage de chaque projet et être pris en compte lors de la contractualisation avec les différents acteurs, la définition de l'architecture et des moyens mis en œuvre et la définition ou l'adaptation des différents processus de l'ensemble des cycles de vie de réalisation, d'exploitation et de maintenance.

Les objectifs de qualité de service DOIVENT porter sur les critères suivants :

- Conditions d'accès à l'espace numérique de travail
- Disponibilité
- Performance
- Intégrité et sécurité des données
- Maintenabilité, Évolutivité et Pérennité

L'atteinte de ces objectifs dépend d'un grand nombre de facteurs. Le tableau ci-dessous présente une liste non exhaustive de tels facteurs, et indique sur quels critères de qualité ils agissent.

	Conditions d'accès	Disponibilité	Performance	Intégrité et sécurité	Maintenabilité
Qualité intrinsèque de l'ENT (facteurs de qualité des composants matériels et logiciels mis en œuvre)					
Dispositifs de sûreté de fonctionnement, tels que la redondance de composants, et des outils d'exploitation mis en œuvre (outils de supervision, consignes de remise en ordre de marche, …)					
Dispositifs de sécurisation de la plate-forme de l'ENT et politique de sécurité					
Efficacité de la chaîne de remontée et de résolution des incidents et des problèmes					
Priorisation des actions de maintenance corrective					
Qualité des formations effectuées au sein des différentes équipes de réalisation, d'exploitation et de maintenance					
Qualité de la formation des utilisateurs et de l'information qui leur est diffusée					
Maintenabilité, évolutivité et pérennité de la solution, à court et à long terme et quelques soient les évolutions des acteurs chargés de cette maintenance (réversibilité) et les évolutions externes influant sur le fonctionnement de l'ENT					
Réactivité des exploitants et des mainteneurs					
Qualité de service des composants externes à l'ENT nécessaires à son utilisation (postes utilisateurs, réseaux, ...) et niveau d'interopérabilité entre l'ENT et ces composants					
Fréquence des évolutions de la plate-forme de production, maîtrise des changements et minimisation des durées et des impacts des coupures de service					
Capacité à remettre en ordre de marche ou reconstituer tout ou partie de la plate-forme de production et de ses données et dans des délais raisonnables					
Capacité à maintenir un bon niveau de performance, malgré l'évolution de la charge d'utilisation, des volumes de données, des évolutions fonctionnelles et technologiques					
Mesures d'actions préventives visant à améliorer la disponibilité, les performances et la sécurité des services					
Qualité de la gestion de projets et de la gestion des risques, aussi bien en phase de réalisation qu'en phase de maintenance					
Niveaux d'engagements contractualisés avec les différents acteurs et répartition des rôles et des domaines de responsabilité					
Contrôles de respect des niveaux de service, analyse des insuffisances et application de mesures incitatives d'atteinte des objectifs fixés					
Mise en œuvre de processus d'amélioration constante de la qualité					
Maîtrise des coûts					

La qualité de service dépend donc d'un grand nombre d'acteurs, ainsi que des moyens mis en œuvre, de la qualité des processus et des contrats signés avec les prestataires extérieurs. Les principaux acteurs qui contribuent à la qualité de service sont :

- les fournisseurs de composants matériels et logiciels standards (constructeurs, éditeurs de progiciels, distributeurs) ;
- les développeurs d'applications spécifiques ;
- l'intégrateur ;
- les mainteneurs des composants matériels, logiciels ou de l'ENT dans son ensemble ;
- l'exploitant ou l'hébergeur, et le centre d'appels ;
- l'équipe de conduite du projet.

Il ne faut pas oublier les utilisateurs eux-mêmes qui, par exemple par manque de compétence ou d'information, ou par manque de discipline notamment lors des périodes de forte charge, peuvent également perturber le fonctionnement de l'ENT (ex : dégradation des performances ou des données) ou de l'activité des exploitants et mainteneurs (ex : signalement de faux incidents).

2.3 Les prestataires et la contractualisation

2.3.1 Principes généraux

Les objectifs de qualité de service DOIVENT être déclinés pour chacun des acteurs et contractants en fonction de leur domaine de responsabilité. Le respect des engagements pris par chacun de ces acteurs DOIT être contrôlé.

Les différents engagements cumulés pris avec les différents acteurs DOIVENT permettre d'atteindre le niveau de qualité de service fixé pour l'ENT. Des engagements personnalisés DOIVENT être fixés pour chacun des acteurs, en fonction de leur domaine de responsabilité. La définition de ces engagements et les moyens de contrôle du respect de ces engagements peuvent être complexes si les contractants sont nombreux ou si les tâches et responsabilités n'ont pas été réparties de manière simple. Il sera par exemple difficile de déterminer la responsabilité d'un acteur dans le cas de dégradation de la disponibilité ou des performances si les composants des services applicatifs, des services socle et des services réseaux ont été répartis dans les domaines de plusieurs prestataires externes. Il sera également, dans ce cas, plus difficile de synchroniser les tâches de ces différents acteurs lors d'évolutions de l'ENT ou du traitement de résolutions d'incidents complexes. Par ailleurs, les organisations, les besoins, les fonctions et les technologies sont amenés à évoluer tout au long du cycle de vie de l'ENT. La flexibilité sera d'autant plus importante qu'il n'y aura pas un niveau d'interdépendance élevé entre les contrats de plusieurs partenaires, leurs moyens techniques et leurs processus.

Il est donc RECOMMANDÉ de limiter le nombre de contrats passés avec des prestataires extérieurs, à charge pour ces derniers de sous-traiter des tâches spécifiques à d'éventuels partenaires. Il est RECOMMANDÉ de désigner un intégrateur global, un mainteneur unique et un hébergeur unique.

2.3.2 Relations entre intégrateur et mainteneur

Les activités d'intégration et de maintenance sont de même nature et requièrent les mêmes compétences. L'intégrateur initial PEUT être retenu pour la maintenance d'un ENT. Dans ce cas, des garde-fous DOIVENT être prévus dans le contrat afin de limiter le risque d'une trop grande dépendance avec le prestataire. Pour cela la clause de réversibilité prévue pour un éventuel transfert de responsabilités à un nouvel acteur dans le cas d'une résiliation ou d'un non renouvellement du contrat DOIT être complétée en prévoyant notamment la réalisation de mesures de contrôle. Ces mesures PEUVENT par exemple s'effectuer au travers de procédures d'audits de la qualité et de la maintenabilité des développements spécifiques, ou au travers de la vérification de la complétude et de l'exactitude des documentations (techniques ou relatives aux processus). Ces documentations DOIVENT être mises à jour au fil des évolutions.

Bien que cela nécessite un effort de transfert de compétences et de responsabilités, la contractualisation avec un mainteneur différent de l'intégrateur d'origine NE DOIT PAS être exclue. Elle permet notamment de s'assurer du bon niveau de maintenabilité de l'ENT et de la non dépendance d'acteurs spécifiques. Il est toutefois RECOMMANDÉ de ne pas effectuer ce changement dès la mise en service de la première version de l'ENT ou d'une des évolutions majeures. Une attention particulière DOIT être portée au transfert de responsabilités vers le nouveau mainteneur, celui-ci devant s'approprier le contexte sans dégradation du degré d'engagement sur le niveau de qualité de service.

2.3.3 Relations entre hébergeur/exploitant et intégrateur/mainteneur

Afin de simplifier la définition des domaines de responsabilité des différents prestataires, il est RECOMMANDÉ de confier toutes les activités d'exploitation à l'hébergeur, y compris l'ensemble de celles relatives à l'exploitation des services applicatifs (ex : optimisation des bases de données, gestion des traces générées par les services applicatifs, …).

Toutefois, les domaines de responsabilité entre hébergeur et mainteneur ne sont pas toujours simples à formaliser, et encore moins, à décliner en indicateurs de mesure contractuels relatifs à la disponibilité et aux performances de l'ENT.

Par exemple, après un incident ayant pour conséquence une rupture de service, l'hébergeur exploitant est responsable de la remise en ordre de marche de ce service. Il est toutefois dans l'impossibilité de le faire si cette remise en service nécessite une action correctrice d'un logiciel, qui est dans le domaine de responsabilité du mainteneur. Dans ce cas, l'hébergeur exploitant DOIT être tenu d'affecter l'incident, de transmettre les informations au mainteneur dans les plus brefs délais et de collaborer pour toute contribution d'analyse de la plate-forme de production.

En ce qui concerne les performances, le partage de responsabilité peut s'avérer relativement complexe. Ainsi, la responsabilité d'une dégradation des performances due à une évolution de la charge ou du volume de données sera difficile à reporter sur un acteur si les ressources des serveurs et des réseaux ne sont pas saturées. L'amélioration d'une telle situation peut nécessiter des actions d'optimisation de services qui sont dans le domaine de responsabilité de l'exploitant (ex : défragmentation du disque, purge de données inutiles, …) ou d'autres actions qui sont dans le domaine de responsabilité de l'intégrateur ou du mainteneur (ex : optimisation des requêtes et traitement des services applicatifs). Il peut arriver que les deux acteurs soient impliqués aussi bien dans l'analyse des causes de la dégradation des performances que dans la réalisation d'actions correctrices (palliatives et/ou définitives). Il est donc important de veiller à ce que les domaines de responsabilité dans le domaine des performances soient décrits avec précision dans les contrats de ces deux prestataires. Il est RECOMMANDÉ de porter une attention particulière à l'étude de dimensionnement que DOIT élaborer l'intégrateur et qui DOIT indiquer précisément les caractéristiques nécessaires de la plate-forme (dimensionnement, paramétrage, …) et les actions que l'exploitant DOIT mener : actions préventives (surveillance, opérations récurrentes d'optimisation et de nettoyage,…) ou correctives (remplacement de composants matériels, paramétrages, changement d'horaires de programmation de batchs, …).

L'exploitation et la maintenance de l'ENT PEUVENT être confiées à un prestataire unique, si ses compétences le permettent, simplifiant ainsi les aspects contractuels. Dans ce cas également, des garde-fous suffisants DOIVENT être mis en place car les risques de perte de maîtrise et donc de dépendance sont élevés. Ces garde-fous se concrétisent par l'attention particulière portée à la clause de réversibilité du contrat, par la possibilité de mener des actions de contrôle et d'audit et par une exigence de transparence minimale au niveau des activités effectuées et des coûts unitaires des devis.

2.3.4 Services standards et spécifiques

Lorsque des offres standards sont proposées (services d'exploitation, plages du service d'accueil, niveaux de qualité de service, ...), elles DOIVENT être comparées aux exigences préalablement définies, et s'en rapprocher le cas échéant, si le rapport entre les services rendus et les coûts de ces services est intéressant.

2.3.5 Propriété des matériels et logiciels

Les matériels et logiciels standards de base PEUVENT être la propriété du financeur de l'ENT, qui signe alors les contrats de maintenance de ces composants. Les exploitants et mainteneurs de l'ENT DOIVENT, dans ce cas, avoir accès au support prévu dans le cadre de ces contrats de maintenance.

Si les composants matériels et logiciels sont la propriété d'un hébergeur, deux solutions se présentent :

- Le prestataire est engagé sur un niveau de qualité de service dans un contexte technique et fonctionnel et sur une volumétrie d'utilisation définis dans le contrat. Il DOIT alerter suffisamment à l'avance le financeur de l'ENT de la nécessité de faire évoluer les composants logiciels et matériels pour maintenir une qualité de service élevée, notamment dans le cas d'évolutions de la charge d'utilisation ou du volume de données, de l'usure des matériels et de la fin de vie (ou fin de support/maintenance) annoncée de logiciels ou matériels. Ce prestataire DOIT de plus indiquer ses recommandations d'évolutions de l'ENT tant au niveau des composants que de la démarche d'évolution (migration, déploiement, …).

- L'évolution des composants logiciels et matériels est à la charge du prestataire, qui DOIT alors effectuer toutes les opérations d'évolution garantissant le maintien d'un niveau de qualité de service élevé, quelque soit l'évolution de la charge d'utilisation ou des contraintes techniques. Le mode de financement de ce prestataire DOIT dans ce cas être adapté en conséquence et, par exemple, être fonction de paramètres de volumétrie factuels (nombre d'utilisateurs déclarés ou simultanés, taille des données, …). Les évolutions de l'ENT DOIVENT être effectuées en cohérence avec l'engagement de qualité de service contractualisé, à charge au prestataire de fiabiliser et optimiser les évolutions afin de minimiser les ruptures de service et les régressions liées à ces évolutions. Le prestataire DOIT être dans l'obligation d'informer l'équipe de maîtrise globale de l'ENT, de manière anticipée, de toute évolution majeure planifiée et de tout risque lié aux évolutions.

En ce qui concerne les droits des développements spécifiques des services applicatifs réalisés par un prestataire extérieur :

- Soit les droits patrimoniaux des développements spécifiques des services applicatifs sont transférés au financeur de l'ENT, à l'issue d'une phase de recette.

- Soit ces droits ne sont pas transférés (cas notamment des ASP, ou « Application Service Provider », qui mettent à disposition des applications en ligne), et le contrat DOIT, dans ce cas, contenir une clause permettant d'assurer la pérennité de l'ENT en cas de défaillance du prestataire ou arrêt de maintenance des logiciels (dépôt des sources, accès aux sources, …).

Il est, par ailleurs, RECOMMANDÉ dans ce cas de s'assurer que la stratégie d'évolution de ces logiciels est compatible avec les contraintes et les besoins prévisibles de l'ENT.

2.3.6 Qualités des prestataires extérieurs et exigences contractuelles

Les prestataires extérieurs retenus DOIVENT respecter notamment les critères suivants :

- Assurer une qualité de service optimum dans la durée.
- Être compétitif, aussi bien en ce qui concerne les prestations récurrentes ou prédéfinies dans le contrat, que les prestations à la demande.
- Être réactif face à une demande d'évolution des services ou de travaux d'exploitation.
- Être en mesure de s'adapter à des changements du contexte, de l'organisation, des processus ou du périmètre.
- Adopter une démarche d'amélioration constante de la qualité.
- Être en mesure de transférer l'activité à un tiers dans des conditions optimales.

Tout contrat avec un prestataire extérieur DOIT pouvoir être résilié pour convenance, pour manquement de l'une ou l'autre des parties ou pour non respect chronique des niveaux de service contractualisés. Le contrat DOIT exiger une garantie de bonne fin, en fin de marché ou après résiliation. Cette garantie DOIT inclure une clause de réversibilité permettant à un tiers de s'approprier l'activité dans des conditions optimales et sans risque de dégradation de la qualité de service ou de la maintenabilité de l'ENT, en exigeant du prestataire initial sa participation pour la migration éventuelle des services de l'ENT sur le nouveau site, et en assurant une continuité de service ou en limitant le temps d'indisponibilité lors du basculement.

Les domaines de responsabilité DOIVENT clairement être établis dans le contrat. Les objectifs de qualité de service DOIVENT être précisés, les indicateurs de mesure NE DOIVENT PAS être ambigus et la méthode de mesure DOIT être définie. Ces indicateurs donnent une vision simplifiée de la qualité de service. Le contrat DOIT donc également contenir des garde-fous permettant de traiter des incidents de prestations ou de sécurité ayant pour conséquence ou pouvant entraîner un incident grave, et précisant un engagement sur un plan d'actions correctives ou préventives.

Un contrat DOIT engager le prestataire à respecter toutes les consignes de sécurité nécessaires et, notamment, sur les aspects de la confidentialité.

Qu'il s'agisse d'un prestataire de maintenance ou d'exploitation, celui-ci DOIT s'engager contractuellement sur des types de prestations prévisibles aussi bien en termes de coûts (unités d'œuvre) que de délais d'exécution, tout en maintenant l'engagement sur les niveaux de service fixés au départ. Cet engagement permet notamment d'obtenir une garantie de réactivité et de maintien des coûts.

Le fournisseur de l'ENT, ou intégrateur, DOIT, sur la base du cahier des charges, justifier les qualités de la solution qu'il propose en termes non seulement de conformité, de fiabilité, de performance et de sécurité, mais également d'évolutivité, de pérennité et de capacité à absorber les évolutions de charge et de volume de données.

3. Les caractéristiques de l'ENT

3.1 Préambule

Afin que les besoins d'exploitation soient pris en compte et opérationnels lors de la mise en exploitation, ceux-ci DOIVENT être définis dans les cahiers des charges de l'intégrateur (puis du mainteneur) et de l'hébergeur.

3.2 Dispositifs de sûreté de fonctionnement

3.2.1 Redondance des composants de l'ENT

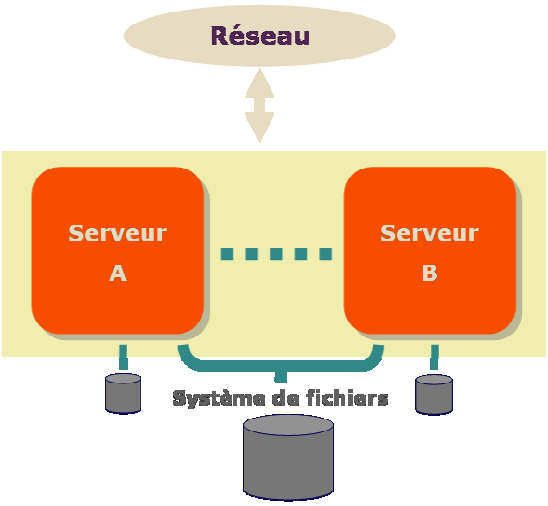
Afin de minimiser l'impact d'un incident grave provoquant une rupture de service, l'ensemble des services réseaux, des services socle et des services applicatifs, tout du moins ceux qui sont jugés les plus importants, DOIVENT être installés sur un système fiable, dont les composants sont redondés et les disques sécurisés. Les machines sont ainsi mises en « clusters » et rendent un service de « haute-disponibilité » en assurant une reprise de tout ou partie de l'activité, après un incident grave, en quelques minutes au maximum.

Des dispositifs de reprise automatique en cas d'incident grave DOIVENT être mis au point et testés avant toute mise en exploitation.

Chaque basculement DOIT provoquer une remontée d'alarme permettant à l'exploitant d'analyser, notamment à partir de la lecture des journaux de traces, la cause probable de l'incident, de résoudre éventuellement cet incident et, le cas échéant, d'escalader cet incident vers un mainteneur tiers de composants matériels ou logiciels.

Un cluster est composé :

- d'un accès réseau, ou point de passage pour l'accès aux machines du cluster à partir de l'extérieur
- au minimum de deux unités centrales de calcul
- des systèmes de fichiers, partagés ou non par les machines du cluster



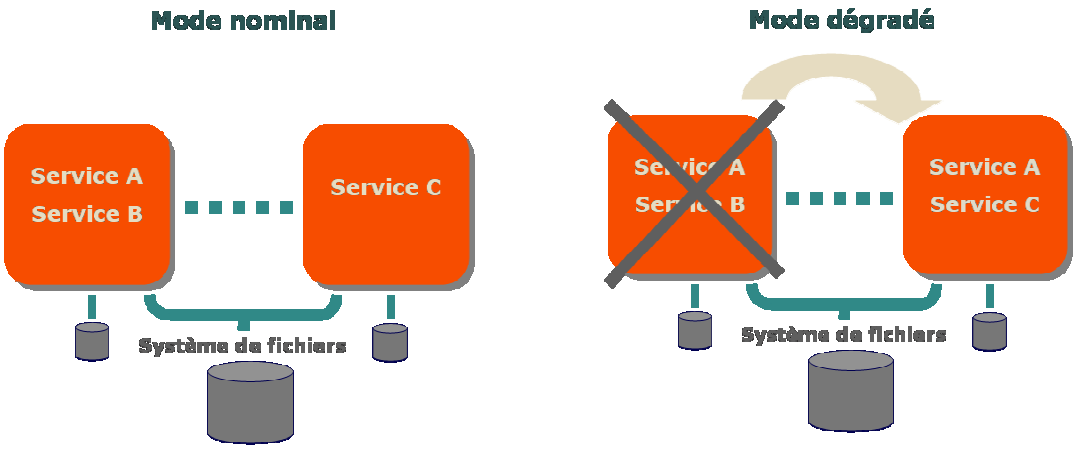
Le basculement automatique ou manuel après un incident PEUT entraîner une dégradation des performances ainsi que la non disponibilité de certaines fonctions moins critiques et jugées comme telles dans le fonctionnement en mode dégradé. Le retour en mode nominal DOIT alors se faire dans les meilleurs délais.

Afin d'optimiser les coûts, les services PEUVENT être répartis sur les différentes unités centrales des machines redondantes. Cet équilibrage PEUT être dynamique ou statique. La redondance des composants doit permettre par ailleurs de répartir la charge en répartissant les services sur les deux unités centrales. Cette répartition peut s'effectuer sur deux modes :

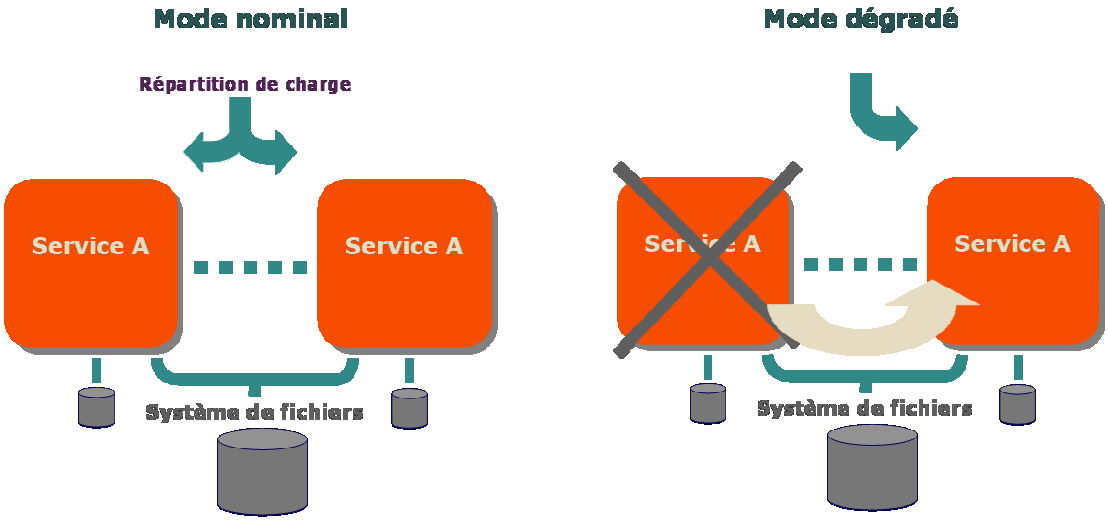
- **Actif-passif** : un service applicatif ne fonctionne que sur une des unités centrales, l'autre n'étant utilisée qu'après un basculement automatique suite à un incident grave ou un basculement forcé pour des raisons de maintenance. Ce mode est simple à administrer. Il permet, de plus, d'installer de nouvelles versions sur le serveur passif, de tester la mise en production avant le basculement en service actif et de basculer pour l'exploitation effective de cette nouvelle version en minimisant l'interruption de service. Les deux unités centrales ne sont pas nécessairement symétriques. Par exemple, l'unité centrale passive peut être de dimensionnement moindre, les performances pouvant être dans ce cas moins bonnes lors des phases en mode dégradé.

  Variante : Il est possible dans ce cas de répartir des services applicatifs différents sur chacune des unités centrales et d'optimiser ainsi le dimensionnement de la plate-forme.

  Dans l'exemple ci-dessous, les services A et C sont des services critiques. En mode dégradé, afin de ne pas trop altérer les performances , le service B n'est pas lancé.



- **Actif-actif** : un service applicatif fonctionne simultanément sur les deux unités centrales. Un mécanisme de répartition de charge permet de répartir les traitements suivant un algorithme prédéfini. Les applications doivent être développées spécifiquement pour supporter ce mode. Le coût de licence des logiciels est généralement plus élevé.



D'autres mécanismes sont proposés par des constructeurs et éditeurs de bases de données (serveur miroir, serveur témoin, ...). Il est RECOMMANDÉ d'effectuer le choix final en fonction des niveaux de disponibilité annoncés, des coûts et de l'évolutivité de la solution. Les solutions de haute disponibilité nécessitent des logiciels supplémentaires. Par ailleurs, les coûts des licences des logiciels de base et de maintenance diffèrent selon la mise en œuvre choisie (actif-passif ou actif-actif).

3.2.2 Sécurisation des fluides

Lors de la procédure de consultation, l'hébergeur devra par ailleurs préciser les autres dispositifs de sécurisation des fluides (électricité, climatisation, réseaux d'accès, ...) et des locaux qu'il mettra en œuvre.

3.3 Surveillance, indicateurs, diagnostic et résolution de premier niveau

3.3.1 Surveillance

Des outils de surveillance, permettant la remontée d'informations sur des incidents et alertes, doivent être mis en place, paramétrés et personnalisés au niveau de chacun des différents composants des services réseaux, des services socle et des services applicatifs.

Ils doivent permettre de remonter vers un ou plusieurs administrateurs :

- des alertes en cas de rupture de service ou d'anomalies de fonctionnement d'un service ou d'une procédure d'exploitation (batch, sauvegarde, ...) ;
- des informations utiles à la résolution d'incidents ;
- des indicateurs pertinents nécessaires pour des actions de maintenance préventive, évitant ainsi une dégradation de la disponibilité ou des performances ;
- des données statistiques, nécessaires par exemple pour affiner le modèle de dimensionnement des composants en fonction de la charge et des usages (en corrélation avec les indicateurs d'usage) ;
- des alertes de sécurité pertinentes ;

- des indicateurs de mesure de la qualité de service globale ou relative au périmètre d'un des acteurs.

Ces outils DOIVENT permettre de définir des gestionnaires d'évènements qui s'exécutent pour une résolution proactive des incidents et la relance automatique de services.

Ils DOIVENT permettre la définition de procédures d'escalade.

Les seuils d'alertes DOIVENT être définis et documentés avant toute mise en exploitation.

Ces dispositifs DOIVENT être complétés par des traces de fonctionnement des services réseaux, des services socle et des services applicatifs, qui seront utilisées à des fins d'analyse d'incidents de fonctionnement ou de sécurité ou à des fins de statistiques.

Les greffons ou développements spécifiques complémentaires DOIVENT être instrumentés pour assurer un bon niveau de traçabilité et de remontée d'indicateurs et alertes de fonctionnement ou de sécurité.

3.3.2 Outils d'analyse

Les ENT DOIVENT être dotés d'outils d'intervention à distance permettant la réalisation de toutes les opérations courantes et urgentes d'exploitation ne nécessitant pas d'opérations manuelles sur site (comme l'introduction de bandes de restauration dans un lecteur). Ces outils DOIVENT notamment permettre de réaliser un diagnostic sur les machines ainsi que la plupart des opérations de maintenance et de relance des systèmes et applications en cas de rupture de service.

3.3.3 Outils de mesure de la qualité de service

Un bon niveau de qualité de service ne peut être obtenu sans indicateurs. Les prestataires extérieurs DOIVENT s'engager sur des objectifs précis de qualité de service, notamment en termes de disponibilité et de performance. Le respect de ces engagements DOIT être contrôlé de manière périodique. Pour cela, les ENT DOIVENT être dotés de mécanismes de mesure capables de fournir des indicateurs de qualité de service en cohérence avec les engagements contractuels. Un mécanisme de calcul de disponibilité d'un service ou de mesure de temps de réponse DOIT être mis en œuvre. Deux principes de fonctionnement sont possibles :

- Mise en place d'un robot jouant en boucle des scénarios représentatifs (un scénario par grande fonctionnalité de l'ENT telle que l'accès à un agenda, …) et mesurant les temps de réponse ou enregistrant, en cas d'erreur, les temps de dysfonctionnements. Cette technique présente l'avantage de pouvoir être utilisée à des points différents du réseau et, notamment, sur des points externes à la plate-forme hébergée. Elle permet d'apprécier ainsi plus finement les temps de réponse du point de vue de l'utilisateur. Elle permet également, en installant le robot en interne, c'est-à-dire sur la plate-forme hébergée, de mesurer les évolutions des temps de réponses en faisant abstraction des éventuelles dégradations dues à une congestion des parties du réseau qui ne sont pas dans le périmètre de responsabilité de l'hébergeur et de fournir ainsi des mesures d'indicateurs contractuels.

- Mise en place de traces au niveau de requêtes représentatives (une par grande fonctionnalité de l'ENT) enregistrant les temps de réponse et les erreurs. Cette technique permet de mesurer les évolutions des temps de réponse et les taux de disponibilité au sein de la plate-forme spécifique de l'ENT. Mais, à la différence du premier dispositif, elle ne permet pas de réaliser des mesures de temps de réponse de bout en bout, ni de tenir compte des périodes de non utilisation des services mesurés. Par ailleurs, les calculs de mesures sur une période donnée sont sensiblement plus complexes.

Ces outils DOIVENT pouvoir remonter des alarmes aux administrateurs en cas de dysfonctionnements ou de temps de réponse fortement dégradés.

Des outils complémentaires permettant le calcul des indicateurs périodiques (mensuels) de qualité de service et de contrôle de respect des engagements des différents acteurs DOIVENT être fournis.

Le paramétrage de ces outils DOIT être documenté. Ils DOIVENT être évolutifs et permettre de réadapter ou enrichir les indicateurs, alertes et traces en fonction des évolutions de l'ENT ou des retours d'expérience.

Les soumissionnaires à une consultation de fourniture de services d'ENT DEVRONT détailler les mécanismes de surveillance et de trace qu'ils prévoient de mettre en œuvre.

3.4 Autres outils d'exploitation

L'ENT DOIT être doté :

- d'outils et de mécanismes automatiques de sauvegardes, d'archivage et de restauration, qui DOIVENT être dimensionnés selon la volumétrie des données à sauvegarder et à archiver et selon les évolutions de cette volumétrie ;
- et de tout autre outil jugé nécessaire pour l'exploitation courante tel que, par exemple, un ordonnanceur de tâches.

3.5 Gestion des configurations

Un outil de gestion des configurations, qui DOIT être mis à jour en permanence, DOIT fournir toutes les informations utiles relatives aux configurations mises en place et à leurs versions. Cet outil est utilisé notamment pour la résolution d'incidents, la maîtrise des processus de livraison et de tests, la reconstitution, le cas échéant, d'une plate-forme et la gestion des licences.

3.6 Gestion des incidents

Un outil de gestion des incidents DOIT être mis en œuvre et utilisé pour l'enregistrement systématique des incidents remontés par les outils de surveillance ou signalés par les utilisateurs.

L'outil de gestion DOIT permettre de gérer le cycle de vie de tout incident et d'assurer notamment, à tous les stades de résolution :

- son escalade aux acteurs responsables selon le niveau de priorité,
- la trace de toutes les informations utiles au diagnostic,
- le suivi de ses évolutions.

Il DOIT également assurer la fourniture d'éléments statistiques permettant d'en suivre la résolution aux différents niveaux de support en rapprochement de la contractualisation le concernant.

Il est fortement RECOMMANDÉ qu'il puisse également gérer une base de connaissance et fournir une aide au diagnostic (ex : arborescence de diagnostic).

Un incident nécessitant une correction dans un ou plusieurs composants de l'ENT, même s'il a été clos après une remise en fonctionnement du service défaillant, DOIT pouvoir être enregistré dans ce

même outil ou un autre outil accessible par le mainteneur de l'ENT. Dans ce dernier cas, il est RECOMMANDÉ de mettre en œuvre une interface de transferts automatiques entre les deux outils.

Par ailleurs, l'outil de gestion des problèmes utilisé pour la maintenance, c'est-à-dire pour la correction des causes des incidents dans des modules logiciels ou matériels, DOIT également permettre d'enregistrer toutes les données utiles pour la mesure des délais de correction et des indicateurs contractuels du prestataire de maintenance.

Il est également RECOMMANDÉ que l'outil de gestion des incidents soit accessible à l'ensemble des acteurs principaux de la chaîne de résolution ou, si ce n'est pas possible, puisse envoyer automatiquement la signalisation de l'assignation d'un incident à un acteur n'y ayant pas accès (message électronique, SMS, …).

3.7 Dispositifs de sécurité

La sécurité de l'ENT doit s'appliquer à différents niveaux :

- Niveau physique : protection de la plate-forme matérielle supportant les services de l'ENT.
- Niveau réseau (ou organisationnel) : cloisonnement des réseaux, filtrage des flux, détection d'intrusion, gestion de listes blanches et listes noires, …
- Niveau logique : protection antivirale, anti-spam, protection des données stockées et échangées, contrôle d'accès des accédants aux services de l'ENT, traçabilité des opérations et transactions, contrôle de contenu, …

Le Ministère de l'Éducation Nationale de l'Enseignement Supérieur et de la Recherche a élaboré un schéma directeur de la sécurité (SDI) et une Annexe Juridique au SDET auxquels il conviendra de se référer pour de plus amples détails.

3.8 Plates-formes

Toute mise en exploitation DOIT être précédée d'une série de tests et de travaux préalables à réaliser sur un équipement composé de plusieurs plates-formes :

- une plate-forme de développement utilisée pour le codage des développements spécifiques et la réalisation des tests unitaires, si l'ENT n'est pas composé intégralement de logiciels standards ou progiciels ;
- une plate-forme d'intégration et de recette, utilisée pour l'intégration des différents modules logiciels, la mise au point d'ensemble, la réalisation des tests fonctionnels et la recette avant la mise en production (VABF) ;
- une plate-forme de diagnostic et de résolution d'incidents et de problèmes ;
- une plate-forme de pré-production, proche de la plate-forme de production et dont la configuration DOIT être similaire à cette dernière, permettant de réaliser les tests de mise en production avant toute migration effective de la plate-forme de production ;
- la plate-forme de production ;
- une plate-forme de formation et de démonstrations (communication).

La plate-forme de production étant redondée, il est possible d'utiliser les composants redondés pour réaliser les tests des phases préliminaires à la mise en production (vérifications du bon

fonctionnement après installation réelle et avant basculement). Cette commodité est applicable sous réserve que les opérations soient effectuées lors de périodes de faible charge et à la condition qu'il n'y ait ni accès aux données réelles, ni risque de perturbation de la qualité de service de l'ENT.

Par souci d'économies, il est RECOMMANDÉ d'étudier plusieurs scénarios possibles d'optimisation de ces moyens notamment lors de la consultation de soumissionnaires.

Un autre exemple consisterait à utiliser la plate-forme d'intégration, ou exceptionnellement celle de pré-production, pour le diagnostic et la résolution d'incidents et de problèmes. Dans le premier cas, étant donné que sur la plate-forme de diagnostic doivent être installées les versions des logiciels en production et sur celle d'intégration les versions des logiciels à mettre en exploitation (versions supérieures), le basculement d'un environnement à l'autre devra pouvoir se faire rapidement (ex : basculement de disques).

Les plates-formes de formation et de démonstrations peuvent être distinctes. Il est possible de faire l'économie de ces plates-formes en utilisant par exemple :

- La plate-forme de production, pour des besoins de formation ou de démonstration de la version « courante » de l'ENT (version en exploitation), sous réserve de précautions préalables notamment en termes de sécurité et de sûreté de fonctionnement : sécurité d'accès aux données sensibles, étanchéité des données réelles (données d'annuaire) et des données factices,, suppression des données factices qui ne doivent pas apparaître dans les archives légales à la fin de la séance, non perturbation des performances, …

- La plate-forme d'intégration, pour la démonstration ou la formation sur une version de l'ENT non encore déployée, sous réserve que les contraintes de planification soient compatibles et que les besoins prioritaires puissent être planifiés de manière fiable.

Dans le cas d'usages multiples de certaines plates-formes, une gestion des priorités DOIT être mise en place afin de ne pas pénaliser la qualité de service. De manière générale, les opérations de résolution des incidents majeurs DOIVENT être prioritaires à toute autre activité. Les plannings des autres projets DOIVENT être adaptés en conséquence.

Un cloisonnement de la plate-forme de production DOIT être mis en place afin d'empêcher le moindre accès aux données de l'ENT à partir d'une des autres plates-formes.

4. Fourniture et évolutions de l'ENT

Afin de fiabiliser la mise en production, d'être en mesure d'atteindre les niveaux de qualité de service fixés et de garantir la pérennité de l'ENT, un certain nombre de directives DOIVENT être respectées en amont de la phase d'exploitation, tant au niveau de la contractualisation, que des livrables et des processus.

4.1 Fourniture initiale

La fourniture initiale d'un ensemble de services est réalisée par un intégrateur chargé, après la mise en exploitation, de maintenir ces services. Cette phase peut se réduire à une personnalisation de solutions standards (ou de progiciels) déployées dans d'autres établissements ou sur d'autres projets.

La fourniture initiale DOIT inclure un ensemble de documentations et de procédures de réalisation, d'intégration, de tests, de mise en production et d'exploitation qui DOIVENT être mises à jour tout au long des évolutions ultérieures dans le cadre des différentes opérations de maintenance.

Dans le cadre de cette phase initiale dans le cycle de vie de l'ENT, et dans le cas de solutions d'intégration, l'intégrateur DOIT mettre au point une procédure de réversibilité, destinée à permettre un changement de titulaire pour la maintenance de l'ENT, à renforcer ainsi le niveau de maintenabilité de cet ENT et à en garantir la pérennité. Cette procédure de réversibilité pourra, par ailleurs, être mise en œuvre partiellement ou intégralement lors de l'affectation de nouvelles personnes dans l'équipe de maintenance et garantir ainsi un transfert de compétences efficace.

La procédure de réversibilité DOIT être mise à jour régulièrement suivant une périodicité prédéfinie (ex : annuellement ou à l'occasion de changement de versions majeures des logiciels).

4.2 Maintenance

4.2.1 Évolution dans le cadre d'une maintenance

La phase de maintenance démarre dès la mise en exploitation de l'ENT, mais la notion d'évolution n'est pas spécifique à la phase de maintenance. En effet, certaines évolutions sont effectuées au cours du cycle de réalisation après l'identification de spécifications incomplètes, de spécifications imprécises et non comprises de manière idoine par l'intégrateur, de besoins affinés à la relecture des spécifications ou de l'observation du fonctionnement d'une maquette, d'évolutions externes (composants standards, …), de nouveaux besoins ou d'inversion de priorités, …

La maintenance matérielle prévoit les remplacements / retraits / ajouts / dépannages d'un équipement ou d'un composant matériel.

La maintenance logicielle prévoit les modifications d'un ou plusieurs composants logiciels (ex : application d'un correctif, changement de version logicielle, modification du paramétrage).

Les opérations de maintenance matérielle et/ou logicielle peuvent être classées en plusieurs catégories.

4.2.1.1 Maintenance corrective

La maintenance corrective vise à mettre en œuvre une procédure ou un moyen technique afin de palier un dysfonctionnement (incident) constaté sur une partie du système d'information.

4.2.1.2 Maintenance adaptative

La maintenance adaptative vise à définir un ensemble d'actions de maintenance en vue d'adapter une partie des services de l'ENT à une modification de l'environnement à venir, interne à l'ENT (ex : évolution d'une version d'un logiciel du système imposée par la politique de maintenance de l'éditeur) ou externe à l'ENT (composant interopérant avec l'ENT : postes de travail externes, réseaux, autres services applicatifs).

4.2.1.3 Maintenance évolutive

La maintenance évolutive a pour objet la mise en place de nouveaux services ou l'évolution de ceux déjà présents, améliorant ainsi les services rendus aux utilisateurs et/ou exploitants.

4.2.1.4 Maintenance réglementaire

La maintenance réglementaire a pour objet d'apporter des modifications permettant de rendre compatibles les services applicatifs avec de nouvelles directives réglementaires. Elle s'apparente à la maintenance évolutive. Les délais de mise en œuvre peuvent être très contraignants (basculement à une date précise ou délais de réalisation courts).

4.2.1.5 Maintenance préventive

La maintenance préventive vise à définir un ensemble d'actions de maintenance (logicielle ou matérielle) ayant pour but de prévenir un dysfonctionnement probable ou possible ou une dégradation du fonctionnement (performances,…).

4.2.2 Contractualisation

La maintenance corrective et certaines opérations de maintenance préventive, telles que les mises à jour des patchs de sécurité, des signatures anti-virus et des actions préventives de maîtrise des performances, DOIVENT faire l'objet de forfaits sur la base des niveaux d'engagement de qualité de service souhaités.

Afin de garantir une bonne réactivité du titulaire et la maîtrise des coûts pour la réalisation des autres activités de maintenance, il est RECOMMANDÉ d'introduire dans le contrat des unités d'œuvre pour la réalisation de ces opérations.

4.2.3 Gestion des changements

Une évolution, quelque soit le domaine de maintenance concerné (corrective, évolutive, …), se traduit généralement par un ou plusieurs changements de la plate-forme d'exploitation.

Les changements effectués lors des différentes opérations de maintenance (ajout, retrait ou remplacement d'un composant, modification de modules logiciels ou de paramétrages, …) peuvent avoir, s'ils ne sont pas maîtrisés, un impact négatif sur la qualité de service (coupures de service, instabilité de fonctionnement, …), sur la maîtrise de l'ENT (dégradation du facteur de maintenabilité, perte de connaissance des changements effectuées, …) ou sur les coûts de projets (mauvaise optimisation des évolutions, surcoûts de non-qualité ou de difficulté d'analyse des incidents par manque de maîtrise des changements, non cohérence , …).

Les changements sont, la plupart du temps, planifiables (« changement planifié ») ; ils ne le sont pas dans le cas d'opérations urgentes (« changement urgent ») telles que la résolution d'incidents graves (maintenance corrective) ou la prévention d'incidents graves lors de l'identification de risques importants (seuils d'alarme, nouvelles vulnérabilités, ...).

Les « demandes standards », c'est-à-dire les opérations prédéfinies, compatibles avec l'environnement de production et dont les coûts et modalités sont également prédéfinies, ne sont pas contrôlées par le processus de gestion des changements. Il s'agit d'opérations « courantes », décrites comme étant permises dans les consignes d'exploitation et, si cela est nécessaire, ayant fait l'objet de tests préalables. Il s'agit, par exemple, d'opérations d'extraction de données, d'opérations d'optimisation des ressources, de changements de l'ordonnancement de batchs, de changements autorisés de paramétrages ou de sécurisation de flux, …

Il est important de trouver un compromis entre les délais de mise en œuvre et la fréquence des changements, excepté dans le cas des changements urgents.

Des processus permettant la fiabilisation de la mise en production, la maintenabilité et la minimisation des coupures de service DOIVENT être définis et appliqués. Toute mise en production, même d'une évolution mineure, DOIT faire l'objet de tests préalables, excepté dans de très rares cas où l'urgence prime (alerte importante de sécurité, …). Toutes les documentations et procédures impactées par les changements DOIVENT être mises à jour, ainsi que les informations de la base de gestion de configurations. Si des changements planifiables impactent la disponibilité de l'ENT lors de périodes d'utilisation ou les modes opératoires des utilisateurs, ces derniers DOIVENT être prévenus au préalable (ex : informations sur le portail ou la messagerie électronique).

Certains changements peuvent nécessiter la mise au point de procédures spécifiques ou l'adaptation de procédures existantes permettant de limiter la durée de rupture de service. Dans certains cas de figure, il est préférable de réaliser le changement en plusieurs étapes ou, dans d'autres, au contraire, de grouper ces étapes (ex : changements matériels et logiciels). La stratégie de mise en place de ces changements DOIT être définie et déclinée tout au long du cycle d'exploitation.

L'opération de changement NE DOIT être close qu'après une courte phase d'observation du comportement de la plate-forme suite à l'application de ce changement. En cas d'insuccès, un plan d'actions correctives DOIT être mis en place. Un retour arrière temporaire ou définitif PEUT être décidé, s'il est techniquement possible de le réaliser (compatibilité de bases, ...).

Les changements importants peuvent nécessiter une organisation en mode projet et l'intervention d'acteurs multiples (mainteneurs, exploitants, experts, ...).

Il convient de catégoriser les changements sous deux angles :

- L'urgence du changement, c'est-à-dire l'urgence d'application d'une correction ou de déploiement d'une évolution fonctionnelle ;
- Le niveau de complexité du changement, nécessitant une organisation et des processus plus ou moins lourds.

La gestion des changements DOIT être sous le contrôle d'une personne désignée, appelée « gestionnaire des changements », faisant partie de l'équipe de maîtrise globale de l'ENT, dont les objectifs sont :

- de s'assurer que les changements sont contrôlés et respectent les procédures normalisées ;
- d'éviter les changements sauvages ou non justifiés ;
- d'assurer une cohérence au niveau des évolutions, les sources des changements pouvant être variées ;
- de gérer les priorités des changements et améliorer ainsi la réactivité pour ceux jugés urgents ;
- de gérer les risques et d'en améliorer leur analyse ;
- de limiter les interruptions de service et de fiabiliser les mises en productions ;
- de faciliter la maintenabilité et la gestion des incidents ;
- d'optimiser les coûts et améliorer la productivité.

Dans le cas du choix d'un prestataire extérieur unique pour l'hébergement et la maintenance, le contrat PEUT préciser un niveau de délégation à ce prestataire pour la gestion des changements liés à des opérations de maintenance corrective ou préventive.

4.3 Les étapes préalables à une mise en exploitation

Les besoins pour les mises en exploitation, l'exploitation, ainsi que les objectifs de qualité de service et les indicateurs contractuels DOIVENT être définis dès le départ et, notamment, avant la contractualisation avec l'intégrateur et avant la phase de conception.

La mise en production d'un ENT ou d'une évolution majeure d'un ENT DOIT être précédée par une phase de tests et de recette (VABF) chargée de valider la solution à déployer, les procédures et outils de mise en exploitation et d'exploitation. Après la recette formelle (VABF), la période de VSR permet de vérifier le bon fonctionnement de l'ENT et son exploitabilité en conditions réelles.

Après la mise en exploitation de l'ENT, et le passage du projet en mode de maintenance, tout changement DOIT alors suivre ce même cycle ou un cycle simplifié en fonction de la complexité et du niveau de risque de ce changement.

Un PAQ (Plan d'Assurance Qualité) DOIT être exigé du fournisseur retenu pour chacune des prestations : fourniture de l'ENT, maintenance et hébergement.

4.4 Livrables

Les livrables fournis lors des phases du cycle de vie de projet d'intégration DOIVENT au minimum se composer de :

- Documentations d'architecture et de spécifications techniques et fonctionnelles, documentation du dimensionnement de la plate-forme, dossiers d'exploitation et toute autre documentation nécessaire à la maintenance de l'ENT.

- Procédures de mise en exploitation et documentations associées : procédure d'installation et/ou de migration, procédures de retour arrière, procédures de vérification du bon fonctionnement après installation ou migration.

- Procédures d'exploitation et documentations associées : surveillance, procédures d'installation et de relance unitaire des services, procédures de reconstitution ou remise en ordre de tout ou partie de la plate-forme, procédures de sauvegardes et de restauration, analyses de traces, aide au diagnostic, …

- Documentations de tests et résultats des tests effectués.

Ces documentations sont destinées notamment aux mainteneurs et aux exploitants de l'ENT. La complétude et l'exactitude de ces documentations DOIT être une des conditions de recette du fournisseur (VABF).

Le mainteneur et l'exploitant DOIVENT garantir la mise à jour de l'ensemble de ces livrables lors de toute action d'évolution. Le processus d'évolution des documents DOIT être inscrit dans celui de la gestion des changements.

Les procédures de réinstallation de tout ou partie de plate-forme NE DOIVENT PAS se limiter à des procédures unitaires d'installation de chacun des composants. Après une opération lourde de maintenance matérielle ou logicielle ou après certains incidents, la remise en fonctionnement de la plate-forme DOIT, dans la majorité des cas, s'effectuer selon un processus préalablement validé afin de garantir une remise en cohérence de la plate-forme en composants et en données tout en limitant le temps d'interruption de service.

Ce processus de remise en fonctionnement consiste en un ensemble de consignes précises et bien décrites à exécuter dans un ordre et un timing établis selon des conditions dûment énoncées.

De la sorte l'exploitant et tous ses intervenants seront à même d'intervenir le plus rapidement possible, notamment dans les opérations non programmées de résolution d'incidents, en appliquant strictement la procédure recommandée, sans avoir à chercher des informations ou faire appel aux mainteneurs et sans risquer de mauvaises manipulations. Les délais de remise en fonctionnement de la plate-forme, incluant le cas échéant les délais de restauration des données, DOIVENT préalablement être estimés.

Les consignes d'exploitation DOIVENT être enrichies au cours de la phase d'exploitation à partir des retours d'expérience dans les domaines de la résolution d'incidents et de la remise en service : optimisation, simplification, etc. L'objectif de ce processus est de diminuer les temps de résolution et les temps d'indisponibilité pour améliorer continuellement la qualité de service des versions stabilisées.

4.5 Tests

Toute mise en production d'une version majeure ou tout changement DOIT faire l'objet de tests préalables sur au moins une plate-forme. Le processus DOIT être adapté à chacune des typologies d'évolution.

Les tests sont conduits par l'intégrateur ou le mainteneur de la solution, à l'exception de ceux relatifs aux évolutions maîtrisées par l'exploitant (ex : application de correctifs de sécurité ou de logiciels de base des systèmes, en relation avec les éditeurs ou constructeurs des composants matériels). Dans ce dernier cas, l'exploitant se DOIT d'informer le mainteneur du résultat des tests et de l'évolution réalisée.

Les tests et la stratégie de tests DOIVENT être documentés.

Lors de changements mineurs concernant notamment les opérations légères de maintenance corrective ou préventive ne faisant pas l'objet d'une recette formelle et dont les risques estimés sont faibles, les tests effectués ont pour objet de tester l'évolution. Le cas échéant, si l'évolution peut avoir des impacts sur d'autres fonctions de l'ENT, ces tests DOIVENT être complétés par quelques scénarios de tests de non-régression représentatifs pré-établis.

Lors de changements moyens ou majeurs, un plan de tests DOIT être établi par le mainteneur. Les tests DOIVENT être composés de tests spécifiques de validation des évolutions et d'une liste soigneusement présélectionnée de tests de non-régression suivant les impacts des évolutions sur les modules existants.

Seules les évolutions réalisées dans le cadre de la maintenance corrective et une partie des opérations de maintenance préventive PEUVENT ne pas faire l'objet de recette formelle (VABF et VSR).

Les tests à effectuer ne se limitent pas à la vérification fonctionnelle des services de l'ENT. Toutes les procédures de mise en exploitation DOIVENT être testées et, notamment :

- les procédures d'installation et de migration ;
- les procédures de reprise en cas d'incidents graves (basculement des traitements sur une des unités centrales du système redondé) ;
- les procédures et enchaînements de procédures (consignes) de remise en ordre de marche manuelle de tout ou partie de la plate-forme de production ;
- les procédures de sauvegardes et de restaurations ;
- les procédures de supervision ;
- les procédures de mise en exploitation et, le cas échéant, de migration, les tests de vérification de la mise en exploitation, ainsi que les éventuelles procédures de retour arrière en cas d'insuccès.

Les tests de non-régression et la stratégie de test DOIVENT, si nécessaire, évoluer en fonction des incidents rencontrés en exploitation et des retours d'expérience.

Des tests de performance DOIVENT permettre de calibrer la plate-forme avant une mise en exploitation, d'optimiser les paramétrages et d'affiner le dossier de dimensionnement de la plate-forme. Des scénarios représentatifs des grandes fonctionnalités seront définis avec la Maîtrise d'Ouvrage et testés unitairement et en charge pendant la campagne de tests. Ces mêmes scénarios seront utilisés pour l'évaluation de la qualité de service en exploitation. Chaque soumissionnaire à la fourniture d'un ENT DOIT préciser dans sa réponse les moyens qu'il prévoit de mettre en œuvre pour la réalisation des tests de performances et le dimensionnement de la plate-forme.

La durée de batchs éventuels DOIT être estimée afin d'optimiser la planification de leur exécution, pendant les périodes de faible charge.

4.6 Définition du planning de déploiement

La mise en exploitation d'un ENT ou d'évolutions majeures DOIT se faire progressivement (ex : déploiement pilote, déploiement généralisé dans un nombre limité d'établissements, généralisation progressive ou groupée dans les autres établissements). Un déploiement ne DOIT pas être planifié lors des périodes critiques ou de forte affluence (ex : rentrée scolaire ou universitaire). Les contraintes calendaires de l'ENT étant nombreuses (marchés publics, fonctionnement des collectivités, délais des prestataires et fournisseurs, niveau de risque de non respect du planning, …) il est RECOMMANDÉ de porter une attention particulière aux aspects contractuels relatifs à la définition des objectifs calendaires et des engagements de planning demandés aux prestataires extérieurs.

4.7 Gestion de projet et des risques en phase de maintenance et d'exploitation

La gestion de projet ne DOIT pas s'arrêter à la mise en exploitation d'un ENT. Elle DOIT se poursuivre lors du cycle de maintenance de l'ENT. La fréquence et l'organisation des comités PEUVENT être adaptées à cette phase. La gestion des changements majeurs PEUT s'inscrire dans l'ordre du jour de ces mêmes comités. Ces comités PEUVENT également traiter les évolutions qui nécessitent l'élaboration de cahiers des charges et de devis des prestataires (ex : maintenance évolutive).

4.8 Audits

L'ensemble des acteurs de réalisation, de maintenance ou d'exploitation d'un ENT DOIVENT pouvoir être audités. Les audits peuvent êtres des audits de sécurité, de qualité des réalisations technologiques (ex : audit du code, audit des procédures d'exploitation ou de mesure des indicateurs, …) ou de contrôle de la qualité des processus mis en œuvre (vérification des processus documentés et/ou de leur application).

4.9 Réversibilité

Pour différentes raisons, la maintenance et/ou l'exploitation de l'ENT DOIVENT pouvoir être transférées à un nouveau partenaire (en fin de marché, ou de manière anticipée dans le cas d'une résiliation). Les modalités DOIVENT être définies dans le contrat.

Une phase de réversibilité DOIT être déclenchée suivant un plan de réversibilité mis au point par le titulaire d'origine. Les deux marchés DOIVENT alors cohabiter pendant une courte phase de transition dont l'objet est le transfert de compétences et le transfert des responsabilités.

Il est RECOMMANDÉ de demander au nouveau titulaire d'établir avant la fin de cette phase une analyse de risques argumentée.

Le plan de réversibilité de maintenance et celui d'exploitation DOIVENT être mis à jour de manière régulière et, notamment, à l'occasion de changements importants.

Le plan de réversibilité DOIT décrire :

- L'organisation à mettre en place

- La répartition des responsabilités
- La structuration de cette phase (étapes, relations entre les étapes et conditions de fin d'étape)
- Les éléments de délais et de contraintes de planning
- La description de l'assistance administrative et technique et du transfert de compétences
- La liste des éléments à transférer

Il est RECOMMANDÉ de vérifier le plan de réversibilité de manière périodique ou lors de changements importants.

5. Exploitation de l'ENT

5.1 Activités d'exploitation

Les activités de l'exploitant se décomposent en plusieurs familles :

- La gestion des incidents
- Les opérations courantes d'exploitation : batchs, sauvegardes, analyses régulières de traces, opérations de surveillance, opérations d'administration, …
- Les opérations exceptionnelles ou projets : participation à un changement majeur, …

Certaines opérations courantes d'exploitation PEUVENT être récurrentes et prédéfinies. D'autres, de la même façon que les opérations exceptionnelles ou projets, DOIVENT faire l'objet de demandes de travaux (DT). Les modalités et le niveau d'engagement de ces opérations DOIVENT être contractualisés. Le prestataire DOIT s'engager sur des délais de réalisation de ces tâches en fonction de la catégorie des demandes de travaux.

Le prestataire retenu DOIT élaborer un Plan d'Assurance Qualité dès le démarrage des prestations qu'il DEVRA mettre à jour selon une périodicité prédéfinie.

5.2 Gestion des incidents et des problèmes

Cette partie s'inscrit dans l'élaboration de la gestion des incidents, et admet comme principal objectif l'amélioration de la fourniture de service de l'ENT dans les établissements en diminuant les impacts des incidents et en minimisant la durée d'interruption d'un service.

5.2.1 Définitions

Incident	Un incident est un évènement opérationnel non prévu, qui ne s'inscrit pas dans le cadre normal d'un service de l'ENT, et qui entraîne ou pourrait entraîner une interruption de service ou encore sa dégradation en terme de qualité.
Problème	Un problème est la cause sous-jacente d'un ou plusieurs incidents.
Erreur connue	Problème dont la cause est connue ou problème ayant une solution de contournement
Solution de contournement	Solution mise en place temporairement ou définitivement, pour résoudre un incident ou éviter un incident, sans que la cause soit connue ou éliminée (correction)

La résolution d'un incident signifie que des opérations ont été effectuées pour une reprise du fonctionnement normal (ex : relance d'un service applicatif). Le problème n'a pas nécessairement été résolu pour autant.

5.2.2 Évaluation de la priorité d'un incident

La classification d'un incident du point de vue de l'ordre de priorité de résolution peut être abordée selon plusieurs axes de réflexion :

- l'importance du service ou de la fonction impactée : par exemple, la non disponibilité d'un service aux utilisateurs est plus grave que celle de certains utilitaires d'exploitation ne mettant pas en péril la qualité de service perçue par l'utilisateur ;

- la gravité : par exemple, un service impacté dont la chaîne applicative admet de bout en bout une redondance matérielle et applicative ne constitue pas une fonction critique. Autre exemple : des désagréments d'ergonomie sont moins graves que la non disponibilité du service ;

- la portée de l'incident : selon la portée, le nombre d'utilisateurs impactés et le périmètre géographique, on accorde plus ou moins d'importance à un incident (ex : un incident sur un poste de travail isolé a moins de conséquence que l'interruption d'un service central, tel que l'annuaire occasionnant la non disponibilité de la quasi-totalité des services pour tous les utilisateurs) ;

- la saisonnalité : elle revêt également un aspect extrêmement important compte tenu des pics de charge journaliers ou saisonniers (ex : conseils de classe pour le scolaire, rentrées scolaires ou universitaires, résultats d'examens et inscriptions pour le supérieur…) ;

- la sensibilité des données concernées.

De ces axes de réflexion découlent la classification de l'incident et la priorité d'affectation des ressources à déployer afin de résoudre dans les plus brefs délais ceux jugés prioritaires.

La classification doit toutefois être simple pour être applicable. Elle PEUT se résumer en trois niveaux de priorité définis ainsi :

Type d'incident	Définition
Bloquant	**Incident rendant le service inopérant** Il concerne un incident généralisé pour lequel il n'existe aucune solution connue de contournement ou palliative. Il concerne également les incidents affectant tous les utilisateurs d'une même entité géographique ou d'un service applicatif.
Majeur	Incident rendant le service inopérant par intermittence sur une partie des données, ou rendant inopérant une fonction importante du service.
Mineur	Incident ayant pour effet d'altérer le fonctionnement du service, mais n'empêchant pas son utilisation.

La classification PEUT être affinée, sous réserve qu'elle soit applicable, en différenciant les services de l'ENT, les périodes,… Une classification simple et facile à appliquer DOIT être privilégiée à une classification plus sophistiquée qui serait alors source d'erreurs ou de négligence car trop contraignante.

Un objectif de délai de résolution des incidents DOIT être fixé contractuellement et sera fonction de la priorité de l'incident et de la période de signalisation (horaires ouvrés ou non ouvrés).

Les niveaux de priorité DOIVENT être liés à des délais de résolution contractualisés avec les prestataires.

Le niveau de priorité DOIT être enregistré dans la fiche d'incident du système de gestion des incidents. Celle-ci peut être amenée à évoluer tout au long du processus de diagnostic et de résolution. Sa valeur DOIT être conservée lors de la clôture de l'incident à des fins de statistiques et de mesures de qualité de service (temps de résolution suivant les priorités).

La priorité d'un incident DOIT être fixée dès la création de la fiche d'incident suivant des critères simples et non ambigus. Si la détermination de la priorité est complexe et dépend de plusieurs critères (ex : service concerné, plage horaire, gravité de l'incident, ...), il est RECOMMANDÉ que celle-ci puisse être en partie automatisée ou que la personne chargée d'en saisir la valeur soit guidée au moment de sa saisie.

Pour pallier le risque de mauvaise classification des incidents, des contrôles par prélèvements PEUVENT être effectués. Toute constatation de mauvaise classification chronique d'un prestataire extérieur PEUT alors faire l'objet d'un incident de prestation et de plans d'actions correctives et/ou préventives.

Les problèmes DOIVENT également être classés suivant trois niveaux de priorité avant d'être affectés aux équipes de maintenance. Exemple de classification :

Type de problème	Définition
Bloquant	**L'incident est bloquant et ne peut être résolu sans la recherche d'une solution de contournement ou la correction de composants** (ex : correction provisoire ou définitive d'un logiciel)
Majeur	L'incident est majeur et ne peut être résolu sans la recherche d'une solution de contournement ou la correction de composants. L'incident est bloquant et a été résolu mais risque de se reproduire si le problème n'est pas résolu efficacement (solution de contournement ou résolution définitive).
Mineur	Autres problèmes

5.2.3 Support

5.2.3.1 Niveaux de support

Le premier niveau de support est déclenché à partir d'incidents remontés par les outils de supervision ou par les utilisateurs qui peuvent utiliser pour cela différents canaux : le centre d'appel et d'autres moyens de communication tels que la messagerie électronique.

Le support est organisé en plusieurs niveaux :

Niveau de support	Tâches liées à l'analyse et à la résolution des incidents
Centre d'appels et Support de niveau 1	Service d'Assistance aux Utilisateurs Premier niveau de diagnostic/résolution d'incidents (questions, difficultés, incidents de fonctionnement…) Gestion / Suivi des tickets d'incident Peut déclencher le support de niveau 2 ou la maintenance
Support de niveau 2 (Spécialistes)	Support ayant un niveau d'expertise plus élevé que le niveau 1 et ayant pour but l'analyse et la résolution d'un incident non diagnostiqué ou non résolu par le support de niveau 1. Peut escalader au support de niveau 3 quand le problème dépasse le niveau d'expertise du niveau 2
Support de niveau 3 (Experts)	Support ayant pour but l'analyse et la résolution d'un incident non diagnostiqué ou non résolu par le support de niveau 2

L'affectation des niveaux aux équipes d'exploitation et maintenance est dépendante de la nature des composants (composants standards ou spécifiques, ...). En général, le dernier niveau est réalisé par le constructeur, l'éditeur de logiciels standards ou le mainteneur de développements spécifiques. Celui-ci est également en charge de la résolution des problèmes, c'est-à-dire des causes sous-jacentes des incidents (ex : erreurs de code logiciel).

La procédure d'escalade fonctionnelle, c'est-à-dire de transfert de la responsabilité de résolution d'un incident ou d'un problème à un niveau de support supérieur, DOIT être documentée.

5.2.3.2 Heures ouvrées

Les heures ouvrées sont à fixer dans le contrat en fonction des exigences de qualité de service des différents services de l'ENT, pour chacun des acteurs du support.

Le **centre d'appels** DOIT fonctionner pendant les heures d'ouverture des établissements et, au minimum, **10 heures les jours ouvrés (8h-18h)**.

Le **support de niveau 1** doit être effectif **24h sur 24, 365 jours par an**, pour prendre en compte au minimum la résolution des incidents bloquants.

Des astreintes PEUVENT être fixées pour le support de niveau 2 et, si nécessaire, de niveau 3 par exemple lors d'opérations complexes (migrations, …) planifiées en heures non ouvrées ou en cas de risques identifiés.

5.2.4 Traitement de l'incident

5.2.4.1 L'identification et la signalisation de l'incident

La création d'un incident a plusieurs origines :

- Détection et remontée d'alerte par les outils de surveillance,
- Signalisation par un utilisateur ou un représentant d'utilisateurs à travers un appel téléphonique ou la diffusion d'informations par messagerie électronique ou par un autre moyen.

Le processus et les moyens de signalisation des incidents par les usagers DOIVENT être définis avant l'élaboration des contrats avec les prestataires extérieurs : moyens de signalisation (assistance téléphonique, messagerie, signalisation directe ou indirecte via un représentant de l'établissement, …) pour chaque profil d'utilisateurs (corps enseignant, élèves ou étudiants, parents d'élèves, …) et en fonction de chaque période (heures ouvrées ou non ouvrées, …).

L'incident, une fois détecté, DOIT être enregistré dans la base de gestion des incidents avec toutes les informations utiles : date et heure de signalisation, détail de l'incident et informations utiles au diagnostic, priorité, ...

Les véritables incidents, liés à des dysfonctionnements de service, DOIVENT être classés dans une catégorie différente de ceux liés à des demandes d'assistance (questions sur un fonctionnement, …) ou à des demandes d'évolution.

L'incident DOIT être suivi jusqu'au rétablissement du service.

5.2.4.2 L'analyse et l'escalade

L'incident PEUT être analysé en ligne (avec l'utilisateur au téléphone) ou en différé. L'ordonnancement des opérations d'analyse et de résolution DOIT être dicté par les niveaux de priorité des incidents.

Si l'incident ne peut pas être résolu par un niveau de support donné, il DOIT être escaladé vers le niveau supérieur.

Le niveau de support responsable de la résolution de l'incident DOIT être indiqué dans la fiche d'incident. Cette information DOIT être conservée après la clôture de l'incident. Les délais

d'assignation d'un incident DOIVENT pouvoir être calculés à partir de l'historisation des différentes dates (signalisation, escalade, clôture). Ils permettront notamment de mesurer les délais moyens de résolution de chacun des niveaux de support.

5.2.4.3 Le rétablissement du service, la résolution de l'incident et la clôture

Le rétablissement du service PEUT se faire :

- Soit par résolution
- Soit par contournement

L'incident est alors clos. Les opérations de remise en service DOIVENT être renseignées. La date de clôture DOIT être enregistrée et permettre de calculer, à posteriori, le délai de résolution.

Un incident peut être clos même s'il n'y a pas eu de rétablissement de service, notamment dans les cas suivants :

- Décision de ne pas traiter l'incident (abandon)
- Faux incident

Si une solution de contournement a été appliquée, sans véritable résolution de la cause de l'incident, une fiche de problème DOIT être créée.

La correction d'un problème PEUT se faire en deux étapes :

- Solution de contournement (palliatif) ou correction provisoire (ex : correction partielle avant diagnostic complet du problème, correction d'attente rapide à réaliser et/ou déployer, remise à niveau de données ou de paramètres, …).
- Correction définitive, de manière isolée ou par inscription dans le contenu d'une version déjà planifiée.

Une fiche de problème peut être close après résolution du problème (erreur connue) ou après abandon.

La correction d'un problème nécessite généralement un changement (diffusion d'un correctif, …) et DOIT donc passer par le processus de gestion des changements. Il PEUT être décidé de ne pas diffuser la correction rapidement.

5.2.5 Reporting

Outre le reporting relatif aux mesures de qualité de service, il est RECOMMANDÉ de mettre en place un reporting automatique pour les incidents :

- des incidents prioritaires hors délais ;
- des incidents dont les délais sont particulièrement longs ;

ainsi que pour les problèmes (mêmes notions).

En effet, même si les mesures de qualité de service sont bonnes et conformes aux objectifs fixés, il est important de veiller à ce que les délais de certaines résolutions et, notamment celles des incidents prioritaires, ne soient pas excessivement longs.

5.2.6 Procédure d'escalade hiérarchique

Une procédure d'escalade fonctionnelle ou hiérarchique PEUT être mise en œuvre lors d'incidents majeurs (fort impact externe) ou dont la résolution ne peut être obtenue dans des délais raisonnables. Un schéma d'escalade définissant les cas de déclenchement de la procédure et les personnes à contacter suivant les périodes horaires DOIT alors être établi. Cette procédure PEUT s'inscrire dans le processus de gestion de crise.

5.2.7 Plan de Continuité de Service

Un Plan de Continuité de Service (PCS) DOIT être mis en œuvre (se reporter au modèle type [6]).

5.2.8 Gestion de crise

La procédure d'escalade fonctionnelle DOIT prévoir en dernier recours une cellule de gestion de crise. Cette cellule est activée dans le cas de difficultés techniques graves, concernant les incidents qui rendent l'ENT indisponible ou qui pourraient le rendre inutilisable s'il n'y était pas remédié rapidement.

Pour ce faire, les responsables des différents systèmes d'information DOIVENT être préparés à ce type d'éventualité.

Le rôle de la cellule de crise est :

- de mettre en place et suivre un plan d'actions urgentes visant à remettre en service l'ENT ou à minimiser le risque d'un incident grave ;
- d'anticiper sur d'éventuelles répercussions que pourrait causer un incident sur l'ENT, par exemple la divulgation de données personnelles d'une ou plusieurs personnes ;
- de minimiser les impacts inévitables par la mise en œuvre d'une campagne de sensibilisation et de prévention (dégradation de l'image de marque, perte de crédibilité, perte de confiance de l'usager, atteinte à la vie privée, …), et surtout par la diffusion de l'alerte ;
- de prendre en charge les mesures adéquates correctives et/ou préventives pour diminuer le risque de reproduction d'un incident similaire.

Les acteurs clés de comités opérationnels DOIVENT faire partie de la cellule de gestion de crise afin de gérer les événements avec efficacité, de poursuivre les actions après la fin de la crise et d'être en cohérence avec toutes les autres actions opérationnelles.

5.3 L'exploitation courante

5.3.1 Journalisation

5.3.1.1 Traces et protection des traces

La journalisation concerne deux types de traces :

- Les traces relatives aux usagers, à l'utilisation de l'ENT et à l'accès aux données, en vue de pouvoir fournir des preuves le cas échéant, et d'être en conformité avec la législation en vigueur (se reporter à l'Annexe Juridique au Schéma Directeur des Espaces Numériques de Travail). Ces traces DOIVENT être archivées.

- Les traces à usage technique permettant de vérifier le bon fonctionnement de l'ENT (surveillance de la Qualité de Service), de compléter les informations relatives aux alertes à incident ou à risque d'incident, et de fournir des éléments d'analyse d'incidents.

Tous les utilisateurs de l'ENT, y compris les administrateurs et exploitants, DOIVENT avoir et utiliser un identifiant nominatif. Tout identifiant de groupe DOIT être exclu. La liste des exploitants ou administrateurs habilités DOIT être mise à jour en permanence. Par exemple, tout départ ou changement de fonction de l'un d'entre eux DOIT être signalé dans les plus brefs délais. Les consignes de sécurité s'appliquent à l'ensemble des acteurs internes ou prestataires extérieurs.

Une journalisation des accès aux ressources et des actions associées, aussi bien des usagers que des personnels techniques (administrateurs, exploitants, …), DOIT être mise en place. Les journaux ainsi constitués DOIVENT impérativement contenir les informations relatives à l'identifiant nominatif, la date et heure de l'accès et les opérations effectuées.

Toutes les opérations d'exploitation (prise de main à distance, sauvegarde, arrêt et redémarrage d'un service, suppression de fichiers, …) DOIVENT être tracées.

Une partie des exploitants ou administrateurs PEUVENT avoir les droits leur donnant un accès aux données des utilisateurs. Ces droits leur sont nécessaires pour réaliser toutes les opérations d'exploitation et de maintenance sur les machines contenant ces données (opérations de sauvegarde, d'archivage et de restauration par exemple). Ces droits ne sont pas destinés à leur permettre une prise de connaissance de données personnelles contenues dans les données de l'annuaire ou dans les données produites par un utilisateur. Ces exploitants ou administrateurs DOIVENT signer une clause de confidentialité leur signifiant l'interdiction de lire ou d'exploiter les données sensibles sans l'autorisation du propriétaire de ces données. Tout accès à ces données DOIT être tracé (ex : opérations de sauvegardes, …). Les exploitants ou administrateurs ayant accès aux données NE DOIVENT PAS avoir accès aux journaux de traces dans lesquels sont enregistrées les opérations qu'ils effectuent. Aucun administrateur/exploitant NE DOIT avoir des accès globaux à la totalité de la plate-forme.

5.3.1.2 Gestion des traces

De façon plus générale, la gestion des traces DOIT s'articuler autour de plusieurs opérations et, notamment :

- L'analyse et la corrélation des journaux de trace en vue d'une procédure de remontée d'incident. La fréquence d'analyse doit se faire en fonction de la criticité du système d'information concerné et de la sensibilité des informations.

- La protection des journaux en confidentialité en définissant précisément les acteurs ayant des droits administratifs sur les journaux et en intégrité en vérifiant les mécanismes générant les traces.

- La sauvegarde, le stockage et l'archivage des journaux en vue d'une restauration éventuelle en cas de panne ou de sinistre.

- La remontée d'alertes en cas d'évènements majeurs mettant en péril la sécurité du système d'information. Le système PEUT, le cas échéant, s'interfacer avec le processus de gestion d'incidents.

- etc.

5.3.2 Sécurisation des données, sauvegarde et archivage

5.3.2.1 Sécurisation des données

La durée de conservation des données en ligne, sauvegardées ou archivées DOIT être en conformité, avec les besoins exprimés, les règles de sécurité, les accords des propriétaires des données personnelles, et la législation en vigueur (se reporter à l'Annexe Juridique au Schéma Directeur des Espaces Numériques de Travail).

Les données sauvegardées DOIVENT être sécurisées :

- En instaurant des accords de confidentialité entre les intervenants, (en particulier entre les prestataires extérieurs et le responsable de l'ENT).

- En instaurant des règles de bonne conduite de l'utilisateur quant aux données à stocker sur l'espace personnel ou les espaces partagés.

- En limitant le nombre de personnes ayant accès aux données sauvegardées, par attribution des droits spécifiques à partir d'un système d'habilitations, et en traçant tous les accès à ces données.

Les administrateurs et exploitants ayant accès aux données DOIVENT, par ailleurs, signer une charte de sécurité qui leur précise qu'ils sont soumis au secret professionnel et à la préservation des informations confidentielles auxquelles ils ont accès. Ils DOIVENT s'engager notamment à :

- ne jamais prendre connaissance des données à caractère personnel des utilisateurs sans l'autorisation de ces derniers ;

- n'autoriser personne à y accéder et ne divulguer aucune information dont ils auraient pris connaissance dans le cadre de leurs fonctions ;

- ne pas se connecter à une ressource (ex : prise de main à distance) sans autorisation explicite de la personne à qui elle est attribuée ;

- intercepter ou interdire tout flux informatique présentant des risques de sécurisé et non utilisé par les services de l'ENT ;

- mener, en cas de menace importante, les actions nécessaires pour en réduire les risques (filtrage de flux, blocage de comptes utilisateurs, …) ;

- ne pas abuser de leurs privilèges et limiter leurs actions aux ressources informatiques dont ils ont la charge dans le cadre de leur mission ;

- ne jamais utiliser leurs privilèges d'administration à la demande de personnes non identifiées et tracer toute demande leur paraissant inappropriée ;

- ne pas contourner les procédures de sécurité établies ;

- ne pas utiliser d'autres logiciels que ceux définis et approuvés dans le cadre de l'ENT ;
- ne divulguer aucune information relative au paramétrage de l'ENT et à l'architecture d'accès aux données à des personnes non habilitées ;
- s'engager à respecter en toute circonstance la législation en vigueur.

5.3.2.2 Stratégie de sauvegarde

Il existe plusieurs manières de réaliser une sauvegarde. Une stratégie de sauvegarde est donc à définir en fonction des données à sauvegarder. Deux critères principaux permettent d'établir une stratégie de sauvegarde : le périmètre des données à sauvegarder et la fréquence des sauvegardes.

La sauvegarde peut être :

- Complète : la globalité des données du serveur ou de l'application est sauvegardée.
- Incrémentale : toutes les données modifiées depuis la dernière sauvegarde incrémentale sont sauvegardées. La sauvegarde complète et l'ensemble des sauvegardes incrémentales consécutives sont nécessaires pour restaurer les données.
- Différentielle : toutes les données modifiées depuis la dernière sauvegarde complète sont sauvegardées. Une sauvegarde complète et une sauvegarde différentielle sont nécessaires pour restaurer les données.

La stratégie de sauvegarde DOIT également intégrer l'ensemble des données :

- Services réseaux, socle et applicatifs : tous les systèmes sont susceptibles d'être restaurés, cela inclut l'ensemble des services, les journaux d'évènements, la définition des seuils et des alertes, toutes les données relatives aux applications ou aux différentes couches applicatives (bases de données)…
- Configuration et paramétrage : toutes les configurations relatives au réseau (switchs, routeurs, proxy…), aux bases de données (configuration des accès…), à l'annuaire (fichier de construction de l'arbre, habilitations des utilisateurs…), …
- Données personnelles et publiques : toutes les données stockées dans l'espace personnel et public des usagers de l'ENT.
- Traces : l'ensemble des traces techniques (journalisation des évènements sur les serveurs et sur le réseau…) et des traces de sécurité (tentatives de connexion au portail, traces relatives aux opérations d'administration et d'exploitation).

Le cycle des sauvegardes DOIT être au minimum :

- Une sauvegarde incrémentale par jour
- Une sauvegarde complète par mois

Les bandes de sauvegardes DOIVENT faire l'objet de tests de vérification.

Un plan de sauvegardes DOIT être établi avant la phase d'exploitation.

La capacité des moyens de sauvegarde DOIT être compatible avec l'évolution de la montée en charge. Les délais de sauvegarde DOIVENT être préalablement estimés.

5.3.2.3 Archivage

L'archivage consiste à historiser les données sauvegardées pour les conserver sur une période déterminée. Le besoin d'archivage DOIT être défini au sein d'un ENT. L'archivage DOIT être une opération déclenchée par son propriétaire ou réalisée avec son accord. Il peut également être lié à des obligations légales de conservation de l'information. L'archivage PEUT utiliser des techniques similaires à la sauvegarde ou être réalisé en ligne, sur d'autres espaces de disques. Les droits d'accès aux données archivées DOIVENT être identiques à ceux des données en ligne.

5.3.2.4 Externalisation

L'externalisation consiste à éloigner géographiquement, dans un esprit de sécurisation, les supports de sauvegarde et d'archivage des supports de stockage des informations de production. Une procédure d'externalisation est en général mise en place pour répondre à un éventuel sinistre sur les installations techniques du système d'information. Les sauvegardes doivent être dupliquées et conservées sur un site de secours avec les mêmes règles de sécurité applicables.

La procédure d'externalisation est une procédure complémentaire à un plan de sauvegarde.

Lorsqu'il y a unicité de données sensibles, c'est-à-dire lorsque celles-ci ne sont pas stockées par ailleurs (papier, autres bases, …), l'externalisation des médias de sauvegarde DOIT être mis en place en définissant une fréquence d'externalisation fonction du niveau de risques.

5.3.2.5 Restauration

Des essais de restauration DOIVENT être réalisés périodiquement.

Les données de production ne peuvent être restaurées sur la plate-forme de production sans l'accord du responsable de données. La restauration s'effectuera notamment en cas de dégradation des données sur la plate-forme de production ou de procédure d'évolution de cette plate-forme (migration logicielle ou matérielle, …). Les données personnelles NE DOIVENT PAS être restaurées sur une autre plate-forme sans l'accord du propriétaire.

5.3.2.6 Destruction des données et rebuts

Une procédure de destruction de données sensibles et de mises au rebut sécurisées des medias contenant des données sensibles (medias de sauvegardes, disques) DOIT être mise en place. Cette procédure est activée :

- Dans le cas d'expiration du délai de conservation de données ;
- Dans le cas de recyclage ou remplacement de matériels (ordinateurs, disques, …)

5.3.3 Lutte anti-virale

5.3.3.1 Préconisations

Une politique de lutte anti-virale DOIT être mise en œuvre.

Du point de vue des « hommes », on distingue trois grands axes :

- La sensibilisation des utilisateurs par le biais de campagnes de sensibilisation au respect des règles d'utilisation des moyens informatiques et au respect des règles comportementales en cas d'infection virale.

- La gestion opérationnelle par la mise en œuvre de l'évolution des processus d'exploitation et de l'infrastructure antivirus.
- L'implication des responsables de l'ENT en contribuant à la gestion de crise et à la sensibilisation des utilisateurs.

Du point de vue des « processus », on distingue quatre grands axes qui DOIVENT être mis en œuvre dans le cadre des ENT :

- La veille et la mise à jour de l'antivirus jouent un rôle prépondérant dans l'anticipation et dans la capacité à réagir en cas d'attaque virale.
- L'évolution de l'infrastructure antivirus a un rôle important dans la capacité de l'infrastructure à intégrer les évolutions et éventuellement à anticiper sur les mises à jour de moteurs (procédures de déploiement, diffusion des signatures…).
- La supervision de l'infrastructure antivirus, c'est à dire la capacité à remonter des alertes et à générer des rapports pertinents sur l'analyse virale.
- La gestion des incidents, à savoir la capacité à s'intégrer dans un processus de gestion des incidents.

5.3.3.2 Mesures de contournement provisoires et permanentes

Dans le cas d'une infection virale de un ou plusieurs composants du système d'information, des mesures correctives DOIVENT être effectuées afin de ralentir la propagation d'un virus, de minimiser l'impact et de sensibiliser les utilisateurs aux risques encourus. Les procédures inhérentes à ce type de contournement DOIVENT être clairement établies.

Les principales mesures qui DOIVENT être appréhendées sont :

- Le cloisonnement des éléments infectés.
- Les mesures d'éradication par la mise à jour des signatures, du moteur antivirus et le nettoyage des données.
- Les mesures de reconstruction, réinstallation des systèmes, procédure de restauration des données.
- L'assistance aux utilisateurs.

5.3.4 Gestion des droits et des flux

Les processus de gestion des droits d'accès aux services et aux données DOIVENT être clairement définis. Les domaines de responsabilité de l'hébergeur et les précautions de sécurité DOIVENT être précisés dans le contrat.

La politique de gestion des flux DOIT également être clairement définie. L'hébergeur ne DOIT réaliser une opération de modification de règles de filtrage (ex : autorisation temporaire ou permanente de transferts de fichiers entre un ordinateur de l'ENT et un ordinateur externe à l'ENT) que dans les cas de figure suivants :

- L'opération fait partie des tâches courantes de l'exploitation. Elle fait donc partie des tâches autorisées dans les manuels d'exploitation livrés ;

- L'opération est exceptionnelle ou correspond à une évolution. Elle DOIT alors être validée par le gestionnaire des changements (et le RSSI, ou Responsable de la Sécurité des Systèmes d'Information) et faire l'objet d'une demande explicite formulée à l'hébergeur.

5.4 Mesures de la qualité de service

Les mesures de la qualité de service DOIVENT porter sur :

- La disponibilité des services de l'ENT
- Les performances de l'ENT
- La réactivité de l'exploitant
- La réactivité du mainteneur
- Le service client

Les indicateurs DOIVENT être :

- Pertinents, et directement reliés à des objectifs jugés importants pour la qualité de service
- Mesurables, les moyens permettant de recueillir les informations étant disponibles et opérationnels
- Rapides à élaborer, pour que l'information ait encore un sens (« fraîcheur de l'information »)
- Sensibles, et permettre de mesurer des variations qui mettent en évidence « au plus tôt » les risques de dérive
- Compréhensibles, la définition des indicateurs et leurs limites étant clairement exposées
- Utilisables, permettant le déclenchement d'actions appropriées en cas de dérive
- Abordables, en évitant la mise en place de moyens sophistiqués ou onéreux

Les indicateurs globaux de disponibilité et de performances DOIVENT être déclinés pour chacun des acteurs en fonction de leur domaine de responsabilités.

5.4.1 Disponibilité des services

Les objectifs de qualité de service des différents services DOIVENT être déclinés en engagements précis et mesurables auprès des différents acteurs de l'exploitation et de la maintenance de l'ENT. Ils doivent se traduire par un taux moyen de disponibilité de services et, le cas échéant, le non dépassement d'une certaine durée d'indisponibilité continue.

La disponibilité des services est mesurée sur une période prédéfinie (par exemple, mensuelle). Les outils utilisés pour les mesures de temps de réponse PEUVENT être communs à ceux de la mesure de la disponibilité. Un service est dit disponible lorsqu'il est actif. Il peut toutefois présenter quelques dysfonctionnements lors de son utilisation, nécessitant des corrections de code et la mise en place éventuelle de solutions de contournements. Ces délais de mauvais fonctionnement ou d'indisponibilité de certaines fonctions du service applicatif ne sont pas pris en compte dans le calcul des délais de disponibilité du service. La disponibilité est ainsi calculée en fonction des périodes où le service est globalement actif.

L'indicateur de mesure DOIT être affecté principalement à l'exploitant chargé de remettre en service au plus tôt un service après un incident ayant eu pour conséquences une interruption de ce service.

Les délais d'interruption de services planifiés (ex : application de changements sur la plate-forme de production) ne sont pas comptabilisés dans les calculs d'indisponibilité.

Ces indicateurs PEUVENT être présentés sous la forme suivante :

Service	Indicateur
Service A	**X_A% (99,xx %) de disponibilité par mois**
Service B	**X_B% de disponibilité par mois**
Service C	**X_C% de disponibilité par mois**

Les valeurs des indicateurs DOIVENT tenir compte de l'impact causé par l'arrêt du service. Ainsi, par exemple, le service de contrôle d'accès devra s'approcher d'un taux de 99,9% (42 min d'indisponibilité par mois), alors que le service de gestion des utilisateurs et de leurs habilitations pourra avoir un taux de disponibilité plus faible.

5.4.2 Gestion et mesure des performances

La gestion des performances recouvre l'ensemble des processus qui permettent de mesurer la performance de sous-ensembles techniques ou la performance du service rendu.

Elle permet notamment :

- D'anticiper les évaluations de la plate-forme pour faire face à des montées en charge par un fournisseur ;
- De détecter les pistes d'optimisation des systèmes et d'amélioration des performances ;
- De mesurer les temps de réponse tels qu'ils pourraient être perçus par un utilisateur ;
- De mesurer les temps de réponse des services d'un fournisseur et contrôler ainsi le respect des engagements de ce fournisseur.

Pour ce faire, l'ENT DOIT disposer d'outils de surveillance permettant de tracer des informations relatives à la consommation des ressources principales (réseaux, mémoire, disque, CPU, ...) et de remontée d'alarmes en cas de dépassements de seuils.

L'exploitant DOIT être en mesure de pouvoir engager des actions correctives ou préventives ou de signaler tout besoin d'évolution du dimensionnement de la plate-forme. Le dossier de dimensionnement de la plate-forme DOIT être mise à jour en fonction des retours d'expérience découlant de l'observation de l'utilisation en grandeur réelle.

La mesure des temps de réponse, comme indiqué plus haut, nécessite la mise en place d'outils spécifiques (robot ou trace des requêtes principales).

Des tableaux de bord mensuels indiqueront les temps de réponse moyens observés par tranche horaire, ainsi que les périodes où ces temps de réponse dépassent un seuil. Les temps de réponses nominaux et le seuil des temps de réponses jugés gênants DOIVENT être définis.

Les contrats passés avec les fournisseurs de service PEUVENT inclure un engagement de non dépassement des délais de ralentissement cumulés sur une période donnée (par exemple, mensuelle).

Les indicateurs PEUVENT être présentés sous la forme suivante :

Service	Indicateur
Domaine fonctionnel A	**X_A% (ou X'_A heures) maximum de ralentissement dans le mois de plus Y_A% par rapport aux temps de réponses nominaux** (Ex : 4h maximum de ralentissement dans le mois de plus de 100% par rapport aux temps de réponses nominaux)
Domaine fonctionnel B	**…**
Domaine fonctionnel C	**…**

5.4.3 Réactivité

5.4.3.1 Délais de résolution des incidents

Les délais de résolution des incidents sont fixés contractuellement avec chaque acteur d'un ou plusieurs niveaux de support.

Ces délais seront fixés par priorité d'incident et PEUVENT se concrétiser sous la forme suivante :

Type d'incident	Engagements	Objectif	Seuil de non-acceptabilité
Bloquant	**4 heures**	**75%**	**2 jours ouvrés**
Majeur	**3 jours ouvrables**	**75%**	**5 jours ouvrés**
Mineur	**5 jours ouvrables**	**75%**	**10 jours ouvrables**

Remarque : les informations contenues dans le tableau ci-dessus sont données à titre d'illustration.

Le calcul de résolution des incidents se basera sur les informations de la base de gestion des incidents. En cas d'intervenants multiples, les délais à prendre en compte sont les délais d'assignation de l'incident à l'acteur responsable de sa résolution.

Les délais anormalement longs d'escalade (avant assignation à l'acteur responsable de la résolution) devront être tracés pour permettre une analyse des causes de ces retards et entreprendre, le cas échéant, des actions correctives.

5.4.3.2 Délais de résolution des problèmes

Des délais de résolution des problèmes devront être fixés contractuellement avec chaque mainteneur de développements spécifiques de l'ENT et mesurés sur les mêmes principes que ceux relatifs aux incidents.

Ces délais seront fixés par priorité d'incident et PEUVENT se concrétiser sous la forme suivante :

Type de problème	Délai de prise en compte du problème	Objectif	Délai de mise en place de la solution à partir du moment où la correction est faite par le mainteneur	Objectif
Bloquant	**4 heures**	**80%**	**2 jours ouvrés**	**80%**
Majeur	**4 heures**	**60%**	**4 jours ouvrés**	**80%**
Mineur	**8 heures**	**80%**	**10 jours ouvrés**	**90%**

Remarque : les informations contenues dans le tableau ci-dessus sont données à titre d'illustration.

5.4.4 Qualité du centre d'appel

La qualité du centre d'appel DOIT être mesurée et contractualisée. Elle PEUT se traduire par :

- une capacité de nombre de prises d'appels simultanés,
- un taux de décroché,
- un taux moyen de temps d'attente,
- etc.

5.4.5 Autres indicateurs

5.4.5.1 Incidents de prestation

Les incidents de prestation, ou erreurs de prestation ayant eu pour conséquence un incident grave de production ou un risque d'incident grave, PEUVENT faire l'objet de mesures contractuelles. Dans tous les cas de figure, ils DOIVENT faire l'objet de plans d'actions pour la mise en place de mesures préventives visant à ne plus renouveler ces erreurs.

5.4.5.2 Incidents de sécurité

Les incidents de sécurité, ou non respect d'une consigne de sécurité, DOIVENT faire l'objet d'indicateurs contractuels avec une tolérance de zéro incident. Tout incident DOIT être sanctionné.

5.4.5.3 Mesures d'efficacité des niveaux de support

Par ailleurs, des mesures complémentaires d'efficacité des différents niveaux de support PEUVENT être effectuées : pourcentage d'incidents résolus par le niveau 1 du support (sans avoir nécessité d'escalade).

Il est très délicat de contractualiser sur ce type de mesures, car l'efficacité d'un niveau de support dépend d'un grand nombre de facteurs externes : la qualité des transferts de compétence par l'équipe de maintenance, l'enrichissement de la base de connaissances par cette même équipe, la qualité des composants mis en exploitation, la volumétrie d'incidents sur une période donnée, ... Toutefois l'analyse de cette mesure peut être riche d'enseignements et permettre d'améliorer les processus de gestion des incidents.

5.4.5.4 Le point de vue des usagers

Il est RECOMMANDÉ de recueillir les observations, réclamations éventuelles et souhaits d'évolution des usagers au travers, par exemple :

- D'enquêtes spécifiques
- De l'organisation de comités d'usagers.

APPENDICE

BIBLIOGRAPHIE

N°	Documents de référence MENESR	Source
[1]	Schéma Directeur des Espaces numériques de Travail	http://www2.educnet.education.fr/sections/services/ent/sdet/
[2]	Annexe « Interopérabilité »	Annexe du SDET sur la définition des standards à suivre et des conditions à respecter pour qu'un ENT soit interopérable avec les autres. http://www2.educnet.education.fr/sections/services/ent/sdet/
[3]	Annexe « Recommandations SUPANN »	Annexe du SDET sur le projet d'annuaires pour les établissements d'enseignement supérieur. http://www2.educnet.education.fr/sections/services/ent/sdet/
[4]	Schéma Directeur de la Sécurité des Systèmes d'information	Organisation et orientation de la sécurité des systèmes d'information pour les communautés éducatives. http://www.orion.education.fr/dpma-a3
[5]	Dossier d'exploitation de l'ENT	http://www.educnet.education.fr/superieur/kit-unr.htm
[6]	Plan de Continuité de Service	http://www.educnet.education.fr/superieur/kit-unr.htm
[7]	Glossaire du SDET	http://www2.educnet.education.fr/sections/services/ent/sdet/