EXPOSE DES MOTIFS ET PROJET DE DECRET

accordant au Conseil d'Etat un crédit d'investissement de CHF 8'631'500 destiné à financer la mise en place de mesures de diminution du risque et du pilotage de la sécurité des systèmes d'information au sein de la DSI

1 PRÉSENTATION DU PROJET

1.1 Résumé

La sécurité des systèmes d'information (confidentialité, intégrité, disponibilité et traçabilité) fait partie de l'une des missions de la DSI. Sa maîtrise passe par la diminution des risques et l'identification suivie du traitement efficace des incidents de sécurité, ceci afin de garantir la qualité convenue du service délivré par l'administration cantonale et donc l'image de professionnalisme associée.

L'ouverture de l'accès des systèmes d'informations aux citoyens, la cyberadministration, fait partie de l'évolution naturelle de notre société à laquelle l'ACV a décidé de s'aligner via l'adoption par le Conseil d'Etat du Plan directeur cantonal des systèmes d'information (SI) en novembre 2009 puis de la stratégie e-VD 2012-2017 de déploiement de la cyberadministration en mai 2012. La volonté d'en assurer la sécurité a été confirmée par l'adoption en juin 2011 de la Politique générale de sécurité des systèmes d'information (PGSSI-VD) dont les 5 axes sont:

1. un système de management de la sécurité conforme aux meilleures pratiques
2. une gestion des risques régulière, efficace et proportionnée
3. des mesures de sécurité conformes aux meilleures pratiques
4. une exploitation et une évolution des SI conformes aux politiques de sécurité
5. une mise en œuvre progressive et pragmatique.

Le programme de législature 2012-2017 publié par le CE en octobre 2012 réaffirme ses orientations en matière d'administration en ligne et d'amélioration de *l'efficience des prestations grâce à des processus administratifs simplifiés et des* ***services informatiques*** *adaptés, performants et* ***sûrs***(mesure 5.1).

En janvier 2010, la DSI s'est dotée d'une unité de sécurité des systèmes d'information (USSI) qui a commencé à réaliser un certain nombre d'actions et à mettre en place des mesures de réduction du risque permettant d'améliorer la sécurité applicative et le traitement des incidents de sécurité. Néanmoins, avec l'ouverture des systèmes d'information vers le monde extérieur, les risques et leurs impacts doivent être pris très au sérieux et la mise en place de mesures de diminution des risques secondé d'un système de management de la sécurité devient incontournable (1 ^{er}axe de la PGSSI-VD).

Le présent EMPD vise à la mise en œuvre de la première phase de la sécurité des systèmes d'information qui permettra à la DSI de diminuer les risques et d'améliorer le pilotage de la sécurité en fonction des principaux risques encourus et de traiter aussi efficacement que possible les

incidents de sécurité. Il s'agit d'un pré-requis indispensable à l'utilisation de la cyberadministration par le citoyen et le respect de la loi sur la protection des données.

En plus d'une première série de mesures de sécurité qui permettent de diminuer les risques en prévenant et en détectant d'éventuelles attaques aux systèmes d'information, le présent EMPD couvre la mise en place des processus d'un système de management de la sécurité de l'information conformément aux meilleures pratiques (normes ISO). Par ces actions, la gestion du risque pourra être réalisée en continu, avec efficacité et proportionnellement aux risques encourus.

L'amélioration de la sécurité des systèmes d'information financée par cet EMPD inclut les ressources financières pour réaliser une analyse des risques la plus complète possible sur les systèmes d'information en vue d'estimer les risques qui n'ont pas encore été pris en compte et de s'assurer de la complétude du périmètre.

A noter que, parmi les mesures de sécurité retenues, un volet important concerne la continuité des activités que l'ACV doit fournir même en cas de catastrophe. L'hypothèse qui a été prise en compte pour ce que la DSI appelle une catastrophe, consiste en une destruction partielle ou complète des systèmes informatiques de l'ACV (par exemple Data center). Pour pallier à ce type de défaillance, il a été prévu de mettre en place un site secondaire offrant la redondance d'un certain nombre d'applications et plate-formes informatiques reconnues comme indispensables par une étude sur la continuité effectuée en 2010. Cette étude sera reprise et complétée pour se baser sur les processus métiers critiques dans le but d'identifier les applications et plate-formes informatiques incontournables pour assurer leur fonctionnement habituel même en cas de catastrophe (plans de secours).

L'investissement pour les premières mesures de sécurité nécessaires à la diminution du risque et un système de management de la sécurité de l'information se montent à CHF 8'631'500.-. La réalisation est planifiée sur environ deux ans.

Les coûts importants de fonctionnement annuels correspondants seront intégrés dans le budget de fonctionnement de la DSI, grâce à une proposition d'optimisation des ressources de la DSI (internalisation).

La sécurité des systèmes d'information pourra être renforcée et complétée dans des phases suivantes, courant 2015, et fera l'objet de nouvelles demandes d'investissements, en fonction du bilan de la première étape et de l'analyse des risques complétée et actualisée.

2 ANALYSE DE LA SITUATION ACTUELLE

2.1 Préambule

En sa qualité de service, la Direction des systèmes d'information (DSI) est en charge de la gestion des systèmes d'information et de télécommunication de l'Administration Cantonale Vaudoise (ACV). Son périmètre de compétences est décrit à l'art. 2 du règlement relatif à l'informatique cantonale (RIC).

Ainsi, la DSI a pour mission d'assurer la disponibilité et donc la sécurité des moyens informatiques et de télécommunications nécessaires quotidiennement au bon fonctionnement de l'Administration et de mettre en œuvre, avec les services bénéficiaires, des solutions contribuant à rendre les processus de l'Administration plus simples et plus efficients, pour elle-même et pour les usagers (c.f. article 6 du RIC).

2.2 But du document

Les objectifs de la DSI décrits dans la carte stratégique sont en phase avec le programme de législature du CE et s'alignent sur ceux du système d'information décrit dans le Plan Directeur Cantonal des Systèmes d'Information 2009-2013.

Dans ce dernier, les cinq objectifs pour le socle du système d'information sont:

1. La modernisation des infrastructures
2. La consolidation des plate-formes prioritaires
3. Le développement et l'ouverture des registres cantonaux
4. Le renouvellement des SI transversaux critiques
5. La mise en œuvre du guichet électronique

Les objectifs 3 et 5 énumérés ci-dessus mettent en avant une ouverture au grand public des systèmes d'information étatiques ; ceci est appelé la cyberadministration. Les autres objectifs concernent l'évolution des systèmes d'information vers une meilleure fiabilité et leur optimisation.

La volonté de cette évolution décrite par le Conseil d'Etat est claire et, dernièrement, l'approbation de la PGSSI-VD confirme son positionnement pour que la sécurisation des systèmes d'information accompagne la mise en place de la cyberadministration. En effet, l'administration cantonale va proposer aux citoyens des services en ligne qui peuvent varier de la simple consultation de la situation fiscale à l'achat de documents officiels comme des actes de naissance. Ces processus doivent non seulement être sans faille mais être sous un parfait contrôle de la part de l'administration cantonale, comme le souligne le programme de législature 2012-2017 du CE, notamment dans la mesure 5.1 qui réaffirme la poursuite du déploiement de la cyberadministration et l'amélioration de *l'efficience des prestations grâce à des processus administratifs simplifiés et des* ***services informatiques*** *adaptés, performants et* ***sûrs***.

Les services de l'ACV ne peuvent pas se permettre d'enregistrer ou de délivrer des informations partielles, voir éventuellement fausses. Ils ne doivent pas non plus donner des renseignements confidentiels aux mauvaises personnes.

L'ouverture vers le monde externe exposera les systèmes à des risques considérables qu'il faut très sérieusement prendre en compte. Etre réactifs sur ces aspects, c'est-à-dire corriger un ou plusieurs problèmes après leur avènement, nuirait très fortement à l'image du service public, le discréditerait et pourrait, suivant la gravité de l'incident, enfreindre la loi sur la protection des données. Pour être proactifs et éviter ceci, il faut se donner les moyens de diminuer les risques en identifiant les menaces potentielles ainsi que les vulnérabilités des systèmes pour pouvoir mettre en œuvre un plan de réduction, de transfert ou d'acceptation de ces risques.

Les informations, ou données stockées au sein des serveurs informatiques de l'ACV, doivent respecter les principes de sécurité (confidentialité, disponibilité, intégrité et traçabilité) et concernent tous les services propriétaires de ces données.

Les principaux risques sont induits par la forte augmentation du nombre d'utilisateurs par rapport à l'utilisation interne actuelle, les problèmes d'identification de la personne qui dépose ou qui lit des informations et la capacité du système dans sa globalité à résister et à répondre à des attaques de personnes malveillantes.

Les audits du CCF et de l'ASSIT ont montré que les systèmes d'information de l'ACV ont depuis plusieurs années grandi plus vite que leur sécurisation et un retard certain a été pris dans ce domaine.

Suite à une enquête menée auprès de certains services, la DSI a identifié un certain nombre d'applications métiers et plate-formes dont la disponibilité est critique. Ces applications/plate-formes font partie d'un programme de mise en place de mesures afin d'en assurer la disponibilité selon les besoins métiers, mais les autres aspects de sécurité (confidentialité, intégrité et traçabilité) n'ont pas encore été pris en compte.

L'analyse de risques effectuée dans le cadre du processus de continuité de l'informatique cantonale a aussi montré l'existence de risques potentiels à fort impact liés à un manque de mise en place de mesures de sécurité.

Fort de ces constats, un document de pré-analyse des risques qui récolte toutes ces informations a

permis de qualifier les risques encourus et de proposer des mesures pour diminuer les risques proportionnellement à leur importance. Ceci dans le but d'assurer au mieux la sécurité des systèmes d'information dans le cadre de l'ouverture des services de l'ACV vers le 'monde extérieur'.

Ceci consiste à:

- Diminuer les risques proportionnellement à leur importance et à leur coût de traitement

Au sein de la DSI la direction des solutions métiers (DSOL) se chargera de continuer l'intégration de la sécurité dans le programme de cyberadministration, la continuation du projet GDIA et la formation à la sécurité des personnes concernées. Le centre d'exploitation (CEI) se chargera de mettre en place le cloisonnement de l'infrastructure, la sécurité des données et de préparer l'infrastructure sur un site secondaire externe afin d'héberger une première partie d'applications et de plate-formes pour en assurer la continuité en cas de catastrophe sur le site primaire. Et enfin, l'unité pour la sécurité des systèmes d'information (USSI) se chargera de la sécurité transversale avec la mise en place d'outils de prévention et de détection d'intrusion, la finalisation et l'intégration de la plate-forme SPIAC et la reprise de l'étude de continuité de 2010 basée sur les applications et plate-formes informatiques pour l'axer sur les processus métier critiques afin d'identifier leurs réels besoins de l'outil informatique en cas de catastrophe.

- Mettre en place un système de management de la sécurité de l'information (SMSI)

Le SMSI permettra à la direction de la DSI de piloter la sécurité.

L'unité pour la sécurité des systèmes d'information (USSI) se chargera de sa mise en place avec les outils nécessaires à son fonctionnement.

2.3 Situation actuelle

Début 2010, la DSI s'est dotée d'une Unité de sécurité des systèmes d'information (USSI) dont la mission est d'assurer la sécurité des systèmes d'information de l'Administration Cantonale Vaudoise (ACV).

Depuis sa création l'USSI a contribué à la réalisation d'un certain nombre d'actions comme l'écriture de la PGSSI-VD qui a été adoptée par le conseil d'Etat en juin 2011, l'écriture de directives de sécurité, l'assistance aux projets métiers pour améliorer la sécurité applicative et le traitement des incidents de sécurité. Ceci a permis d'améliorer quelques aspects de la sécurité des systèmes d'information, mais les moyens limités n'ont permis que d'adresser les fonctions de base de la sécurité sans pouvoir diminuer des risques importants. Aujourd'hui l'USSI a de grandes difficultés pour identifier si une attaque aux systèmes d'information est en cours et n'est pas non plus toujours en mesure de gérer un incident de sécurité.

En plus, comme cité dans la section précédente (*2.2 But du document*), une pré-analyse des risques montre que les systèmes d'information de l'ACV présentent un nombre conséquent de failles relativement importantes.

Une telle situation, surtout dans le cadre de la mise en place de la cyberadministration, ne serait pas acceptable. Par exemple une ou plusieurs personnes malveillantes pourraient réussir à accéder à des informations sans même que l'on puisse le détecter, laissant libre cours à leurs actions.

Les situations les plus graves pouvant être envisagées sont:

- le vol de données sensibles (lecture et/ou copie)
- la modification ou la perte des données (destruction)
- l'indisponibilité des systèmes informatiques.

Lorsque l'exploitation de l'informatique cantonale était externalisée, une des faiblesses identifiées était l'absence de site secondaire. Depuis la reprise des activités d'exploitation au sein de l'ACV en août 2009, la situation n'a pas évolué sur ce point. Ceci implique qu'en cas de catastrophe (inondation,

incendie, etc…) provoquant la destruction des serveurs du centre de calcul de la DSI, les services métiers dépendant de l'outil informatique pour effectuer leur travail se retrouveraient dans l'impossibilité d'assurer leur mission pendant plusieurs semaines.

2.3.1 Conséquences

Les conséquences de ces situations peuvent être graves, voire désastreuses pour l'ACV.

Atteinte à la confidentialité : la lecture ou la copie de données sensibles, qui pourraient être potentiellement publiées, se traduirait directement par:

- la perte de confiance du citoyen dans l'ACV
- la perte d'image de la qualité des services délivrés par l'ACV
- la violation possible de la loi sur la protection des données
- une éventuelle crise politique.

Atteinte à l'intégrité : la modification ou la perte des données se traduit directement par des coûts supplémentaires tels que:

- les coûts directs associés à la restauration des données
- si la restauration n'est pas possible:
  - les coûts d'un travail pouvant se chiffrer à plusieurs années*homme de la part du ou des services métiers touchés, pour tout vérifier et remettre en état les données
  - les coûts pour redemander des informations au citoyen qui, comme dans le cas des données sensibles, signifierait une perte de confiance dans l'Administration.

Atteinte à la disponibilité : l'indisponibilité des systèmes informatiques se traduit directement par des pertes et des coûts supplémentaires tels que :

- les coûts directs associés à la gestion de l'incident de sécurité

· Les heures de travail perdues (si 1'000 collaborateurs de l'ACV ne peuvent pas travailler pendant 2 jours (16 heures), ce sont donc 16'000 heures de travail de perdues, soit environ 8 années*homme).

· La perte d'image de la qualité des services délivrés par l'ACV

- La perte de revenu (par exemple, retard sur des encaissements ou des paiements).

Parmi les autres conséquences importantes pour l'ACV, surtout en cas d'impossibilité de reprendre rapidement les activités critiques en cas de catastrophe, on peut rajouter des dommages indirects tels que :

- les heures de travail perdues (si 8'000 collaborateurs de l'ACV ne peuvent pas travailler pendant 30 jours (240 heures), ce sont donc 1'920'000 heures de travail de perdues, soit environ **1'000 années*homme**)

· L'indisponibilité, voire la perte de données à des moments clés, en particulier pour les prises de décision et la délivrance de prestations engageant l'Etat:

- le non-respect des obligations légales (délai)
- les conséquences médiatiques (atteinte à l'image et à la crédibilité de l'ACV)
- la perte de confiance des partenaires et entreprises
- la perte de confiance des usagers (internes et externes)

ou encore la perte de confiance et de motivation des collaborateurs.

2.3.2 Conclusion

Pour la DSI, suite aux risques majeurs identifiés et conformément à la volonté du Conseil d'Etat d'y remédier, il devient indispensable de maîtriser dans sa globalité la sécurité des systèmes d'information. Ceci ne peut se faire qu'en évaluant et gérant les risques en diminuant les vulnérabilités, en surveillant les systèmes informatiques et en récoltant les traces d'audit associées. Même si la sécurité absolue n'existe pas (un incident peut toujours survenir), il est important d'atteindre un niveau de sécurité plus adapté.

En considérant:

- les constats de la situation actuelle et de leurs conséquences
- les exigences découlant des évolutions inscrites dans le Plan directeur cantonal des systèmes d'information 2009-2013, notamment les évolutions en matière de cyberadministration et la mise en place de la sécurité
- la Politique générale de sécurité des systèmes d'information (PGSSI-VD) adoptée par le CE
- la nécessité de la réduction des risques décrits plus haut tant sur les usagers internes (productivité) qu'externes (population, entreprises, partenaires),

Il est indispensable :

- de mettre en place ou d'améliorer les systèmes et les applications permettant de diminuer les risques en fonction de leur importance au niveau:
  - des solutions métiers (DSOL)
  - de l'exploitation et des infrastructures (CEI)
  - de la sécurité transversale (USSI).
- de mettre en place un système de management de la sécurité de l'information (SMSI) qui, en plus de gérer la coordination et l'évolution des systèmes de sécurité, permet de récolter les informations, les filtrer et les mettre sous forme de tableau de bords pour pouvoir les transmettre à la direction de la DSI. Celle-ci pourra ainsi piloter la sécurité.

3 CONTENU ET LIMITES DU PROJET

3.1 Vue d'ensemble de la cible

La pré-analyse des risques qui, comme décrit dans les sections précédentes, se base sur des audits, une récente analyse des risques sur la continuité, les constats sur le terrain et les applications/plate-formes identifiées comme les plus critiques, a déjà permis de mettre en évidence des failles de sécurité d'une certaine importance. Les principaux risques liés à ces failles ayant été identifiés et qualifiés, ils sont pris en compte dans cet EMPD dans le cadre du processus "traitement des risques" dont le rôle est de mettre en place des mesures pour diminuer le risque proportionnellement à son importance.

La sécurisation des systèmes d'information du canton va donner la possibilité de remonter les informations au centre de sécurité opérationnel et se concrétisera par la mise en œuvre de mesures de sécurité telles que la prévention et la détection d'intrusion. La récolte de ces informations va permettre de mettre en place la traçabilité, de générer des tableaux de bords, de produire des statistiques et de gérer les incidents de sécurité.

Cette mise en place va se dérouler de manière itérative en tenant compte des risques les plus importants avec l'application des mesures adéquates et selon les meilleures pratiques.

Une autre mesure de diminution des risques va se concrétiser par la mise en place d'un site secondaire qui va permettre d'héberger les applications et les plate-formes qui sont utilisées par les services de l'ACV pour assurer leurs missions en cas de catastrophe et qui sont considérées comme critiques selon

les critères validés par le Conseil d'Etat. Ceci est une longue démarche qui doit se faire en plusieurs étapes et plusieurs années pour que sa réalisation aboutisse au succès.

La coordination de tout ceci sera assurée par un système de management de la sécurité de l'information qui est un ensemble de processus qui vont être intégrés dans le système de management de la DSI. Ces processus vont permettre de mettre en place une organisation de pilotage de la sécurité des systèmes d'information en fonction des risques encourus et la gestion des incidents de sécurité.

Lorsque le SMSI sera fonctionnel, le pilotage de la sécurité sera effectif. La direction de la DSI sera ainsi informée:

· sur une base régulière de la situation et de l'évolution de la sécurité des systèmes d'information

· en temps réel en cas d'incident de sécurité qualifié de 'grave'.

Cette démarche donne la possibilité à la DSI de construire la sécurité des systèmes d'information de l'ACV d'une façon cohérente, progressive et selon les meilleures pratiques.

Une analyse des risques globale sur la sécurité des systèmes d'information n'ayant jamais été réalisée, il est important au niveau du processus "analyse des risques" du SMSI de partir sur une base solide. Cette analyse des risques, qui demande un effort important, sera donc effectuée dans le cadre de cet EMPD. Elle va permettre non seulement de réévaluer les risques déjà identifiés, mais en plus de découvrir tous les risques mettant en danger l'informatique cantonale qui héberge les systèmes d'information de l'ACV. Ces risques seront catégorisés et, en fonction de leur importance, pris en compte pour être traités avec un ordre de priorité dans les phases suivantes.

4 ETUDE D'ALTERNATIVES DE SOLUTIONS

Compte tenu de sa capacité à réaliser et de l'importance à répondre aux besoins prioritaires définis dans la section 2.2 (*But du document*), la DSI souhaite :

· diminuer à un niveau acceptable les risques principaux identifiés par la pré-analyse des risques

· mettre en place un SMSI (système de management de la sécurité de l'information).

4.1 Variante A - Statu quo

Maintenir la situation actuelle expose les systèmes d'information à des risques considérables et non maitrisés. En plus elle ne permettrait pas à la DSI d'assurer la sécurité des systèmes d'information de manière adéquate conformément à sa mission de base, comme définie dans le règlement de l'informatique cantonale. Cette dernière est indispensable au fonctionnement de l'ACV. Le statu quo aggraverait les insuffisances constatées, notamment dans les évolutions planifiées d'ouverture des systèmes d'information au grand public (cyberadministration) et ne permettrait plus à la DSI d'assurer la gouvernance de l'informatique cantonale.

En plus, en l'absence d'indicateurs de sécurité et d'outils de détection d'intrusion appropriés, la DSI ne sera en mesure ni d'atteindre les objectifs de sécurité issus des évolutions demandées dans le Plan directeur cantonal des systèmes d'information 2009-2013, ni de répondre aux décisions et orientations du Conseil d'Etat (PGSSI-VD, programme de législature 2012-2017).

4.2 Variante B - Réduction de tous les risques identifiés, mise en place d'un SMSI

En tenant compte des évolutions demandées dans le Plan directeur cantonal des systèmes d'information 2009-2013, la DSI pourrait choisir de mettre en place un SMSI avec des mesures de diminution des risques sur tout risque connu, qu'il soit critique, important ou mineur.

Ceci, non seulement ne serait pas aligné avec le 2 ^{e}et 5 ^{e}axe de la PGSSI-VD (2 ^{e}axe : gestion des risques régulière, efficace et proportionnée ; 5 ^{e}axe : mise en œuvre progressive et pragmatique), mais en plus cela donnerait l'impression illusoire d'avoir un système de sécurité sans failles et qui aurait un

coût nettement plus élevé que la variante C.

Il y aurait même le risque que la DSI, avec les moyens dont elle dispose, rencontre des problèmes de surcharge de travail pour mettre en place des mesures de sécurité sans valeur ajoutée.

4.3 Variante C - Retenue par la DSI – Réduction des principaux risques identifiés, mise en place d'un SMSI

Compte tenu des évolutions demandées dans le Plan directeur cantonal des systèmes d'information 2009-2013 et des décisions du Conseil d'Etat (PGSSI-VD), la DSI a choisi de diminuer les risques les plus critiques et de mettre en place un SMSI.

Les mesures permettant de diminuer les risques, et le SMSI avec ses processus décrits dans cet EMPD, sont évalués et limités à leur périmètre strictement obligatoire.

Dans la première phase la diminution des risques sera limitée à ceux identifiés comme les plus importants par la pré-analyse des risques et proportionnelle aux risques encourus. L'analyse des risques, qui sera effectuée dans le cadre de cet EMPD, va permettre d'identifier les risques liés à l'informatique cantonale et de les catégoriser en fonction de leur importance. Ceux-ci seront pris en compte dans les phases suivantes avec une mise en place des mesures de diminution des risques proportionnée aux risques encourus. Cette procédure itérative tient compte de la capacité de la DSI à réaliser et de l'expérience acquise.

La surveillance et le traitement des incidents de sécurité seront effectués dans le cadre du SMSI par un centre de sécurité opérationnel dont le périmètre de travail sera fonction de celui défini par le traitement/diminution des risques.

Cette variante a l'avantage de réduire les risques et de prévoir la mise à disposition de processus, de procédures et d'outils de sécurité opérationnels et de pilotage pour la DSI, dans le but d'optimiser la détection, la prévention, le traitement des incidents de sécurité et le reporting pour la direction. L'industrialisation du processus de changements permettra d'intégrer immédiatement la sécurité des applications et de leurs données associées. A terme, ceci permettra d'assurer une cohérence sécuritaire globale.

La mise en place efficace et réaliste de la continuité des activités en cas de catastrophe passe par une étude des processus métier critiques dont l'outil informatique est incontournable à leur fonctionnement, ce qui va permettre d'identifier les vrais besoins de redondance de l'informatique sur un site secondaire. Dans cette variante, en plus de cette étude qui va développer les plans de continuité à réaliser, on va commencer à mettre en place l'infrastructure et les premiers éléments connus comme indispensables pour assurer la continuité des activités des processus critiques. La mise en œuvre complète des plans de continuité sera assurée par des projets ultérieurs (étape 2).

5 SOLUTION PROPOSÉE

La solution proposée (variante C) se décompose de la manière suivante:

- Diminution des risques:
  - mise en place des mesures de sécurité, y.c. en matière de plans de secours
  - analyse des risques
  - formation
- SMSI:
  - mise en place des processus composant un SMSI selon ISO 27001 et ISO 27005:
    - pilotage
    - analyse des risques
    - traitement des risques
    - contrôle de l'efficacité

    - gestion des incidents de sécurité
    - gestion de la documentation et de la preuve
- Formation et sensibilisation:
    - mise en place d'un centre de sécurité opérationnel
    - gestion des incidents de sécurité

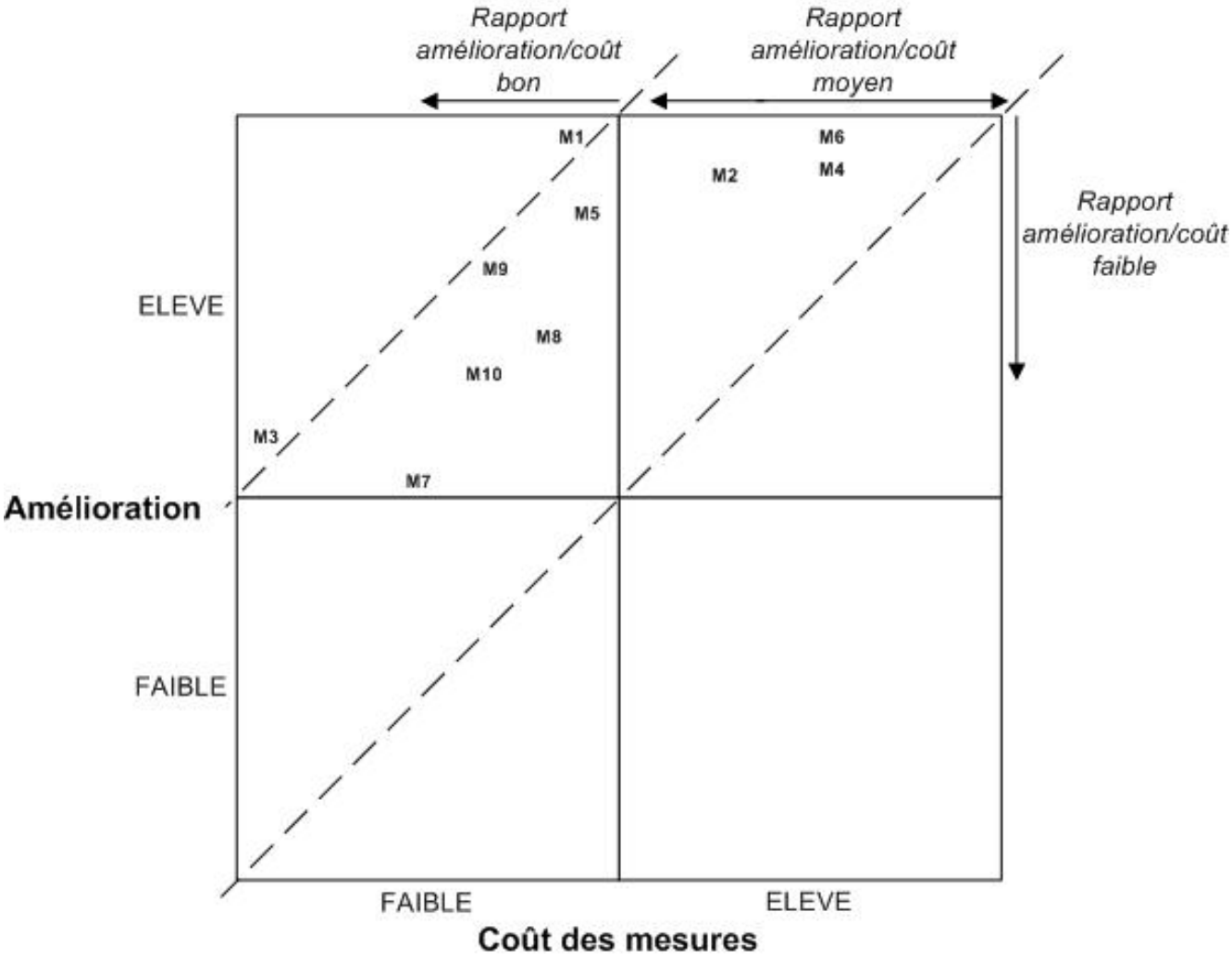
5.1 Projet de diminution des risques

Le tableau ci-dessous établit la correspondance entre les mesures de diminution de risques proposées dans cet EMPD et les risques identifiés dans la pré-analyse des risques.

	Mesures EMPD	**Risques selon document de pré-analyse**
M1	Prévention et détection d'intrusion	- Hackers externes - Virus - Absence de mécanisme de détection d'intrusion
M2	Sécurité des données	- Sécurité des serveurs
M3	Intégration SPIAC	- Sécurité physique - Renforcement des contrôles d'accès physiques
M4	Intégration GDIA	- Droits d'accès aux systèmes d'informations - Mauvaise gestion des droits d'accès
M5	Intégration de la cyberadministration	- Hackers externes
M6	Cloisonnement de l'infrastructure	- Gestion des droits d'accès administrateur - Droits d'accès aux systèmes d'informations - Différence de sécurité des serveurs - Contrôles d'accès réseau - Absence de segmentation des serveurs du Data Center - Non anonymisation des données de production - Mutualisation aveugle des ressources - Sécurité des serveurs
M7	Formation	- Manque de formation - Encadrement des mesures cryptographiques
M8	Processus SMSI	- Manque de procédures pour certaines opérations liées à des travaux sur la production - Virus - Droits d'accès aux systèmes d'informations - Mutualisation aveugle des ressources - Encadrement des mesures cryptographiques
M9	Centre de sécurité opérationnel	- Virus - Sécurité physique - Renforcement des contrôles d'accès physiques
M10	Gestion des incidents de sécurité	- Hackers externes - Virus - Sécurité physique - Absence de mécanisme de détection d'intrusion

Le graphique ci-dessous contient les mesures de diminution du risque financées par cet EMPD (Mx).

Elles sont placées en fonction de leur coût et de l'amélioration de la sécurité obtenue. Ainsi on peut observer aisément l'efficacité de la mesure (amélioration) par rapport au coût de sa mise en œuvre.



5.1.1 Mise en place des mesures de sécurité

La diminution des risques n'est possible qu'avec la mise en place de mesures de sécurités. Ces dernières sont soit des systèmes permettant la prévention (pro activité), soit des systèmes permettant la détection (réactivité). Dans les deux cas, les informations ou alarmes issues de ces systèmes permettent de savoir ce qui se passe et donc de prendre les décisions de sécurité adéquates. C'est le pilotage de la sécurité.

Sur la base de la pré-analyse des risques, la DSI a pu identifier ses besoins en mesures de sécurité afin de diminuer les risques. Ces mesures de sécurité se divisent en deux groupes:

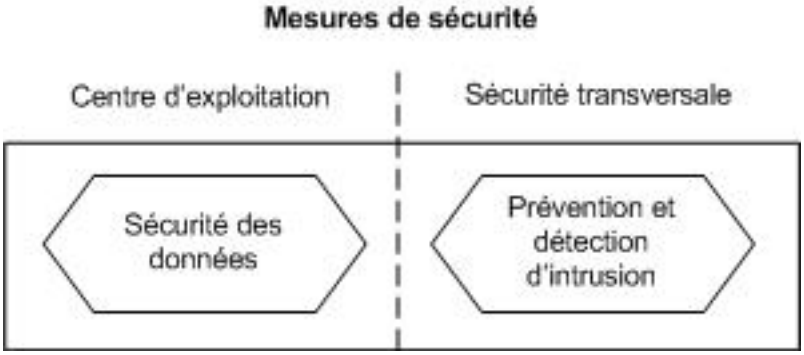
· Amélioration ou mise en place de systèmes de sécurité

Ce sont des composants qui permettent:

- la détection d'un comportement anormal (surveillance et, en cas de comportement anormal, émission d'alarme)
- la prévention d'un comportement anormal (surveillance et, en cas de comportement anormal, blocage et émission d'alarme)
- la sécurisation d'un ou plusieurs éléments sensibles.

Les deux premiers cas de figure enregistrent les informations afin de pouvoir remonter dans le temps et comprendre la raison ayant déclenché l'alarme.

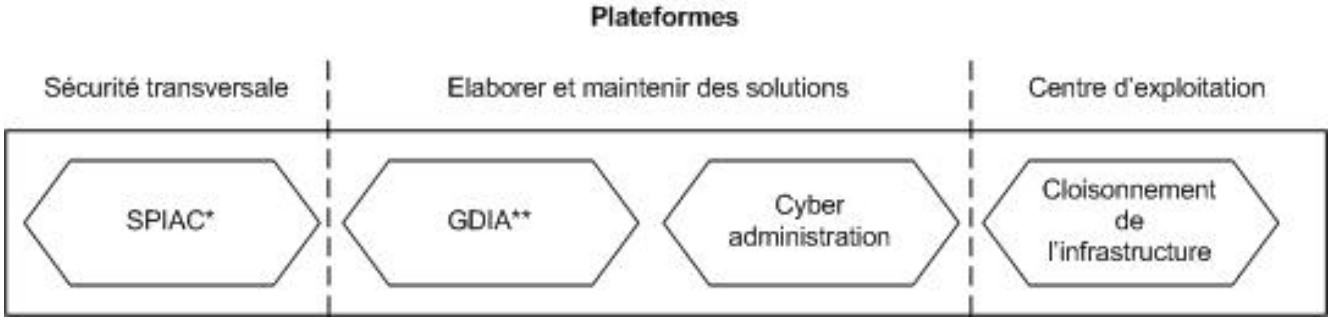
Le graphique ci-dessous représente les mesures de sécurité préconisées:



· *Utilisation des informations des plate-formes existantes ou à créer*

La majeure partie ce sont des plate-formes existantes dont les informations très utiles n'attendent que d'être exploitées. En ce qui concerne le cloisonnement de l'infrastructure, la nécessité de sa mise en place est un élément clé pour assurer une sécurité plus robuste et surtout uniforme.

Le graphique ci-dessous représente les plate-formes préconisées:



* Sécurité Physique des Installation de l'Administration Cantonale

** Gestion Des Identités et des Accès

5.1.1.1 Mesures de sécurité

Dans cette première phase la DSI va procéder à la mise en place des composants suivants :

· *Prévention et détection d'intrusion (IDS / IPS)*

Un certain type de systèmes seront connectés aux points stratégiques du réseau cantonal vaudois (RCV) afin de permettre de détecter les intrusions (surveillance IDS). Un autre type de systèmes consiste à empêcher les intrusions en les bloquant (IPS).

La prévention d'intrusion doit être utilisée avec circonspection de manière à ne pas rendre des services indisponibles ou gêner leur fonctionnement.

Toute information de détection d'intrusion et de blocage sera transmise au SIEM.

· *Sécurité des données*

Dans le cadre d'une stratégie de défense en profondeur, la base de données est le dernier élément à défendre car elle se trouve en bout de chaîne. Comme c'est elle qui contient les informations qui, suivant les cas, peuvent être très sensibles, son importance peut être capitale.

Des solutions permettant d'assurer la sécurité de ces bases existent et doivent être déployées pour assurer une cohérence de la sécurité que l'on veut mettre en place au niveau des systèmes d'information de l'ACV qui sont hébergés au CEI.

5.1.1.2 Plate-formes

L'utilisation des informations des plate-formes existantes ou à créer se décompose de la façon suivante:

· *Intégration SPIAC*

La plate-forme SPIAC (Sécurité Physique des Installations de l'Administration Cantonale) gère actuellement la sécurité des accès physiques de 4 sites. Le déploiement de cette plate-forme est en cours et devrait couvrir progressivement tous les sites de l'ACV. Toute information récoltée sera transmise au SIEM.

Le périmètre du projet SPIAC reste identique à celui défini actuellement.

· *Renouvellement de composants et intégration GDIA*

Le programme GDIA (Gestion des Identités et des Accès), initié par la DSI en 2010, vise la plate-forme IAM en vue d'améliorer la sécurité des données et des systèmes, et d'assurer la montée en charge liée notamment aux utilisateurs de la cyberadministration.

Les volets couverts par le présent EMPD et liés à la thématique GDIA sont :

§ le renouvèlement des briques obsolètes de la plate-forme IAM

§ la mise en place des traces d'audit requises par les directives de sécurité.

· *Intégration de la cyberadministration*

La cyberadministration par sa nature va pousser à l'exposition des systèmes d'information de l'ACV sur Internet avec tous les risques que cela comporte.

La mise en place future de chaque application métier sur le socle de la cyberadministration va devoir suivre une démarche permettant d'assurer une structure sécuritaire de réduction des risques.

· *Cloisonnement de l'infrastructure*

Le modèle de sécurité en vigueur actuellement se base sur un découpage en zones réseau qui convient bien à une administration fermée dont l'informatique s'adresse exclusivement à ses employés et à une époque où la mobilité n'était qu'un concept.

Aujourd'hui, pour faire face à l'évolution du public cible de l'informatique qui s'ouvre vers le citoyen avec la cyberadministration, ce modèle ne suffit plus. Il devient indispensable d'évoluer vers un modèle où les privilèges sont liés à une personne dûment identifiée et authentifiée quel que soit le périphérique sur lequel elle travaille et quelle que soit la zone réseau d'où elle se connecte.

Ce nouveau modèle prend en compte 3 axes:

§ le cloisonnage des zones d'hébergement des serveurs

§ le découpage des données

§ le découpage des rôles et responsabilités.

5.1.1.3 Plans de secours

· *Premières mesures de continuité*

L'étude de la continuité des activités réalisée en 2010, basée sur les applications et les plate-formes informatiques, a été faite sur les informations connues par les chargés d'affaires internes de la DSI qui sont en relation avec les services de l'ACV. Cette étude a permis de mettre en évidence un certain nombre d'applications et de plate-formes critiques pour lesquelles il faut mettre en place un système redondant sur un site secondaire afin de pouvoir assurer leur fonctionnement même en cas de catastrophe.

Cet EMPD finance la mise en place sur un site secondaire de l'infrastructure et d'un certain nombre d'applications et de plate-formes telles que le réseau, Domino / Lotus Notes, l'active directory, LDAP et les serveurs d'impression (liste non exhaustive).

· *Etude des processus métier critiques*

En cas de catastrophe, l'ACV se doit de pouvoir continuer à proposer au citoyen les services

administratifs minimaux et indispensables. Pour cela, il faut identifier les processus métier critiques. Une fois ces derniers identifiés, on peut déterminer si l'outil informatique est indispensable pour leur permettre de continuer à fonctionner. Si oui, le besoin de continuité informatique est avéré et des mesures pour en assurer son fonctionnement en cas de catastrophe doivent être prises.

Cette étude va se dérouler en 3 phases:

1. L'analyse d'impact métier

La première phase de la démarche consiste à identifier les processus des services ou offices qui utilisent les applications métier définies comme critiques par la DSI. La deuxième phase consiste à identifier des processus métier qui seraient critiques et qui utilisent l'outil informatique d'une manière incontournable pour leur fonctionnement. Les chefs des différents départements, en fonction des services ou offices qu'ils gèrent, devront déterminer quels processus sont réellement à considérer comme critiques.

Seuls les processus qui auront été qualifiés de critiques et utilisant l'outil informatique d'une manière incontournable seront définis et décrits (caractère indispensable, temps admis de pertes de données, temps admis pour la reprise des activités, …). Pour des raisons de disponibilités de ressources, la DSI ne va se focaliser que sur les besoins informatiques qui sont essentiels en cas de catastrophe pour les processus métiers critiques.

2. Analyse des risques de continuité

Seuls les processus métier critiques dont l'outil informatique est indispensable à leur fonctionnement feront partie de cette analyse. Celle-ci va identifier et décrire les mesures de réduction du risque informatique à appliquer aux processus métier qui n'ont pas d'autres solutions palliatives de secours en cas de catastrophe.

3. Plans de continuité informatique

Chaque plan de continuité va décrire précisément la mise en place des mesures de réduction du risque avec leurs coûts et va planifier leur déploiement en tenant compte de l'environnement et du déploiement des autres plans de continuité. Ces plans seront garants de la prise en compte des besoins exprimés par chaque processus métier critique, surtout en ce qui concerne le respect du temps admis de pertes de données et du temps admis pour la reprise des activités.

A la fin de cette étude, la décision sur les plans de continuité informatique à déployer en cas de catastrophe va permettre de définir les moyens nécessaires pour leur mise en œuvre (étape 1 et étape 2).

5.1.2 Analyse de risques

Dans l'état actuel, grâce à la pré-analyse des risques, la DSI est consciente d'un certain nombre de risques potentiels qu'il faut diminuer. Néanmoins, cette pré-analyse, même si elle permet de mener un certain nombre d'actions qui vont améliorer la sécurité des systèmes d'information, n'est pas exhaustive et ne peut pas servir de base de travail pour une amélioration continue.

L'analyse de risques financée par cet EMPD sera itérative et permettra non seulement de réévaluer, mais en plus d'identifier les risques encore inconnus aujourd'hui, et de les traiter chacun proportionnellement à son impact. Ensuite, les risques résiduels pourront être estimés et acceptés.

5.1.3 Formation

Les scans de code source et les audits techniques doivent être des éléments qui confirment la qualité du code applicatif produit et qui devraient faire ressortir, dans le pire des cas, des failles de sécurité mineures.

Pour atteindre cette qualité qui va faire diminuer non seulement les risques mais aussi les coûts, (en

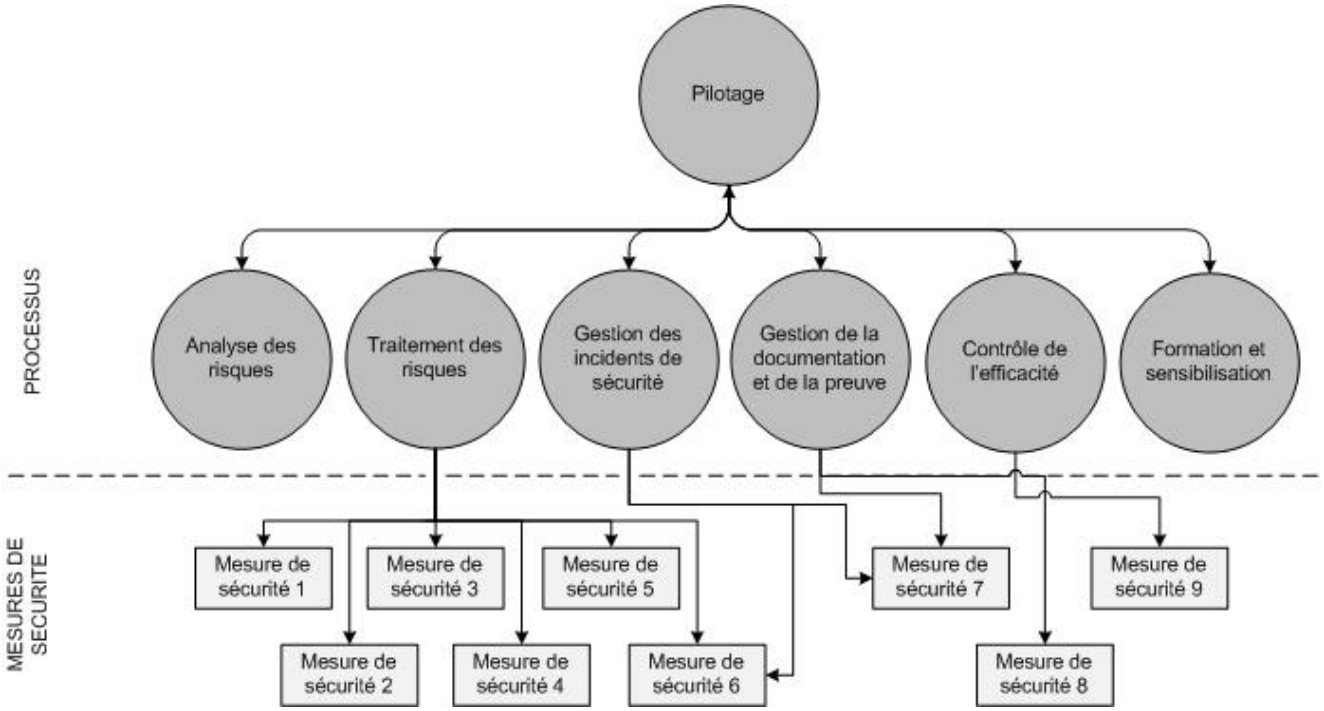
effet, il est reconnu que plus vite on corrige les erreurs, moindre est le coût), la formation est une étape incontournable. Donc, la formation sur la sécurité pour les chefs de projets, les architectes et le personnel interne faisant partie des équipes de développement est un élément essentiel pour la solidité de l'architecture et du code applicatif.

5.2 Projet SMSI

Le but du SMSI (Système de Management de Sécurité de l'Information) est de permettre à la DSI de piloter la sécurité informatique. Sa construction **s**e base sur la mise en place des processus le composant et la mise en œuvre de façon coordonnée d'une sélection pertinente de mesures de sécurité définies dans la norme ISO 27002.

La DSI pourra, en s'alignant sur les principes contenus dans les normes ISO 27001 et ISO 27005, assurer la gestion du SMSI, son contrôle et son amélioration permanente. Naturellement, les processus du SMSI seront intégrés dans le système de management de la DSI.

Le graphique ci-dessous montre les processus d'un SMSI. Il faut noter que les mesures de sécurité représentées sont mises à titre indicatif et leur nombre n'est pas exhaustif.



En plus de la mise en place du SMSI, ce projet comporte les actions suivantes:

· La mise en place d'un centre de sécurité opérationnel

Le centre de sécurité opérationnel, appelé SOC (Security Operation Center) dans le milieu informatique, aura la vocation de collecter, d'analyser et de traiter les événements de sécurité affectant les systèmes d'information de l'ACV. Le centre de sécurité opérationnel est, comme son nom l'indique, la partie opérationnelle du SMSI et ses buts seront de permettre:

- une surveillance et un enregistrement en temps réel des événements de sécurité affectant les systèmes d'information de l'ACV
- la prise de décisions sur la base d'informations fiables
- le contrôle direct de certains éléments de sécurisation et l'envoi d'alarmes
- la gestion des incidents de sécurité
- l'analyse à postériori d'événements affectant la sécurité
- la production de rapports et de tableaux de bords.

· La gestion des incidents de sécurité

La récolte de toutes les informations qui sont délivrées par les systèmes, composants et plate-formes décrits dans la section précédente (5.1 Projet de diminution des risques), va permettre d'identifier d'éventuels incidents de sécurité et de les gérer de la manière la plus efficace possible.

La gestion des incidents de sécurité se fait à l'aide d'outils spécialisés.

Les composants permettant de récolter les informations et de gérer les incidents de sécurité sont :

- le SIEM
- les outils de gestion des incidents de sécurité.

6 COÛTS DES SOLUTIONS

6.1 Coûts d'investissement

Plan d'investissement des différents projets liés au présent EMPD:

En Francs

Projets et sous-projets	Matériel	Logiciels	Prestations	Formation	Total
Diminution des risques					
→ *Mesures de sécurité*					
→ Prévention et détection d'intrusion		160'000	210'000		370'000
→ Sécurité des données		300'000	480'000		780'000
→ *Plate-formes*					
→ Intégration SPIAC		50'000	75'000		125'000
→ Renouvellement de composants et intégration GDIA	140'500	326'000	750'000	120'000	1'336'500
→ Intégration Cyber administration			247'500		247'500
→ Cloisonnement de l'infrastructure		780'000	450'000		1'230'000
→ *Plans de secours*					
→ Premières mesures de continuité	150'000	150'000	200'000		500'000
→ Analyse d'impact métier			750'000		750'000
→ Analyse des risques de continuité			80'000		80'000
→ Plans de continuité informatique			1'200'000		1'200'000
Analyse des risques			150'000		150'000
Formation SMSI				277'500	277'500
→ *Processus composant le SMSI*			465'000		465'000
→ *Centre de sécurité opérationnel*	60'000	150'000	150'000	30'000	390'000
→ *Gestion des incidents de sécurité*					
→ SIEM		200'000	150'000		350'000
→ Outils de réponse aux incidents de sécurité		200'000	180'000		380'000
Total EMPD	**350'500**	**2'316'000**	**5'537'500**	**427'500**	**8'631'500**

En plus de ces investissements, un montant de CHF 1'120'000 sera pris en charge par le crédit d'inventaire.

6.2 Justification de la demande de crédit

Le présent EMPD se justifie par la volonté du Conseil d'Etat de mettre en œuvre le Plan directeur des systèmes d'information de l'ACV et atteindre l'objectif de la mise en place d'une sécurité indispensable avant de procéder au déploiement de la cyberadministration.

L'analyse de la situation actuelle (*Section 2.3*) montre les conséquences potentiellement néfastes du manque de sécurité.

Ces dernières années des entreprises technologiques comme Sony et Nintendo, des banques

comme Citygroup et HSBC ont subi des attaques informatiques ou divulgation de données sensibles qui ont provoqué non seulement une perte d'image considérable, mais aussi des pertes financières très élevées.

Les administrations n'ont pas non plus été épargnées, comme le sénat des Etats-Unis, la CIA et plus proches de chez nous le DFAE et le Service des renseignements de la Confédération. La perte d'image et de confiance auprès du citoyen est difficile à chiffrer, mais implique une méfiance envers l'utilisation de la cyberadministration.

Les estimations montrent que l'investissement pour assurer et maîtriser la sécurité des systèmes d'information est indispensable non seulement pour une question de rentabilité, mais aussi pour une question de réputation et d'image auprès de la population.

6.3 Calendrier de réalisation et de l'engagement des crédits

6.3.1 Principaux jalons

Diminution des risques

- *Mesures de sécurité*
  - Sécurité des données

03.2013 : démarrage de la mise en place
04.2014 : début opérationnel

  - Prévention et détection d'intrusion

03.2013 : démarrage de la mise en place
01.2014 : début opérationnel (périmètre limité)

- *Plate-formes*
  - Intégration SPIAC

06.2013 : démarrage de la mise en place de l'intégration
10.2013 : fin de l'intégration

  - Remplacement de composants et intégration GDIA

03.2013 : démarrage de la mise en place de l'intégration et du remplacement des composants
06.2014 : fin de l'intégration et du remplacement des composants

  - Intégration de la Cyberadministration

03.2013 : démarrage de l'assistance en sécurité
12.2014 : fin de l'assistance en sécurité

  - Cloisonnement de l'infrastructure

03.2013 : démarrage de la mise en place

07.2014 : début opérationnel

- *Plans de secours*
  - Premières mesures de continuité

03.2013 : démarrage
12.2014 : fin de mise en place des premières mesures de continuité

  - Analyse d'impact métier

03.2013 : début
03.2014 : fin

  - Analyse des risques de continuité

04.2014 : début
06.2014 : fin

  - Plans de continuité informatique

07.2014 : début
06.2015 : fin

Analyse des risques
- 03.2013 : début
- 07.2014 : fin

Formation
- 06.2013 : début
- 06.2015 : fin

SMSI
- *Processus composant le SMSI*

03.2013 : démarrage de la définition et de la mise en place des processus
07.2014 : fin de mise en place partielle des processus

- *Centre de sécurité opérationnel*

03.2013 : démarrage de la mise en place
10.2013 : démarrage du fonctionnement

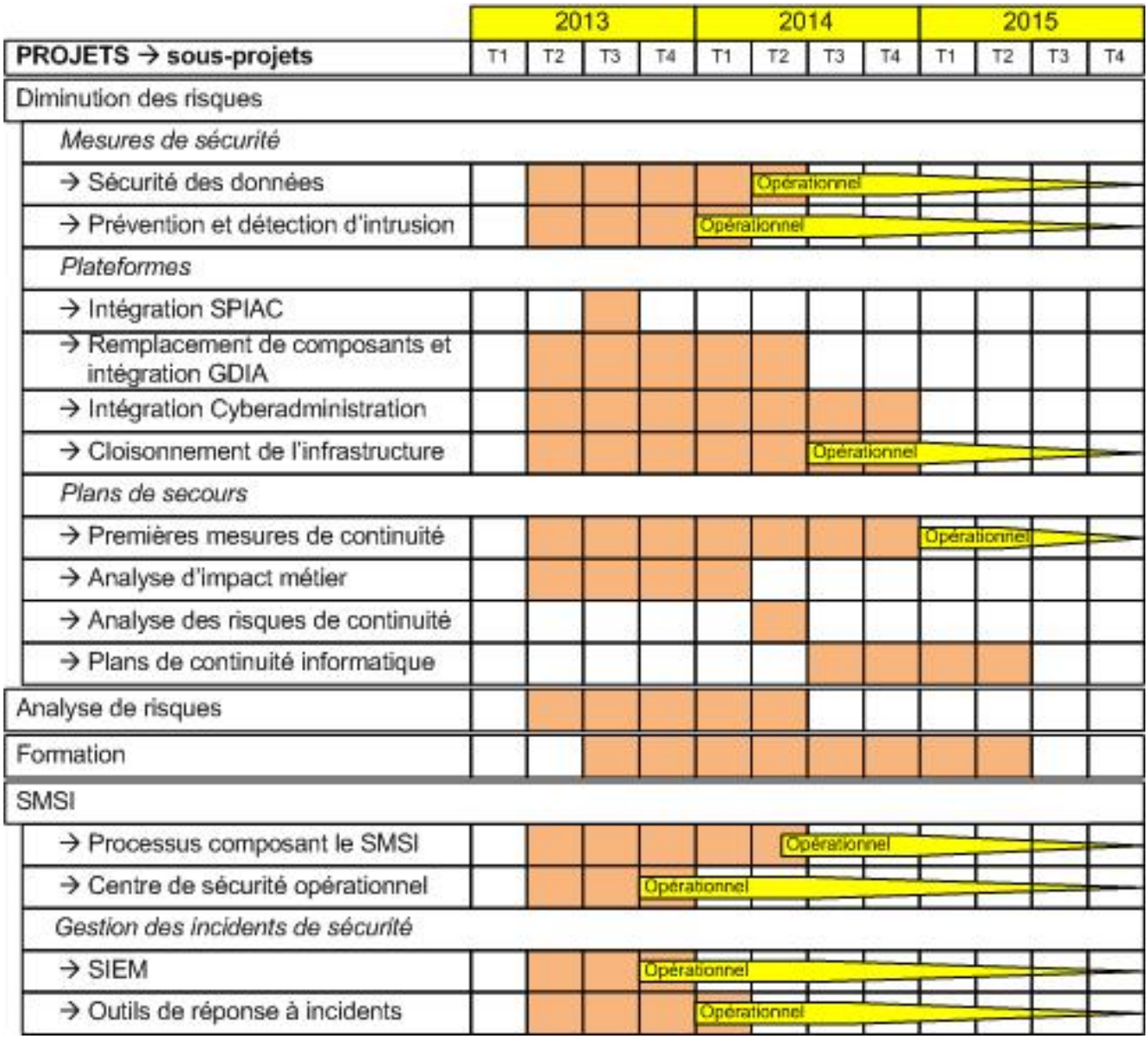
- *Gestion des incidents de sécurité*
  - SIEM

03.2013 : démarrage de la mise en place
10.2013 : début opérationnel sur périmètre restreint

– Outils de réponse aux incidents de sécurité

03.2013 : démarrage de la mise en place
01.2014 : début opérationnel

Le diagramme suivant résume la liste des tâches décrites ci-dessus. Les phases de mise en œuvre des différents composants de la sécurité des systèmes d'information sont grisées. Après cette période, le début opérationnel marque le début de la maintenance corrective et évolutive qui va permettre de répondre à de nouveaux besoins. On peut remarquer que parfois un chevauchement est présent entre ces deux phases. Ceci représente le temps nécessaire aux réglages et à la correction des 'problèmes de jeunesse' pour obtenir un fonctionnement optimal.



Planning de mise en oeuvre

6.3.2 Planification financière (tranches de crédit annuelles)

En prenant comme base les coûts décrits dans la section 6.1 (Coûts d'investissement) et la planification des différents projets, les tranches de crédit annuelles prévues sont les suivantes:

En milliers de CHF	**Tranches de crédit annuelles**			
Années	2013	2014	2015	Total
TCA	3'900	4'000	731,5	8'631,5

Ces tranches de crédit annuelles sont révisées (en cours d'année et lors du processus budgétaire annuel) en fonction de l'avancement des projets et des ressources financières disponibles.

7 MODE DE CONDUITE DU PROJET

- Pour les différents projets de sécurisation du SI de la DSI proposés dans cet EMPD, la DSI est maître d'ouvrage et maître d'œuvre. Les travaux sont donc pilotés par la DSI en impliquant les fournisseurs concernés par les solutions à mettre en œuvre.

L'organisation de chaque projet comprend un comité de pilotage issu de la direction de la DSI, une direction de projet et une équipe de projet dont les membres sont internes (DSI) et externes (fournisseurs).

L'avancement de chaque projet est régulièrement porté à la connaissance du comité de pilotage ad hoc.

Au sein de la DSI, la mise en œuvre est confiée aux entités suivantes en sachant qu'une collaboration sera faire entre tous les acteurs concernés :

· Direction des Solutions métiers (DSOL) pour les projets :

- Diminution des risques
  - Plate-formes
    - Remplacement de composants et intégration GDIA
    - Intégration de la cyberadministration
  - Formation

· Centre d'Exploitation Informatique (CEI) pour les projets:

- Diminution des risques
  - Mesures de sécurité
    - Sécurité des données
  - Plate-formes
    - Cloisonnement de l'infrastructure
  - Plans de secours
    - Premières mesures de continuité

· Unité de Sécurité des Systèmes d'Information (USSI) pour les projets:

- SMSI
  - Processus composant le SMSI
  - Centre de sécurité opérationnel
    - SIEM
    - Outils de réponse aux incidents de sécurité
- Diminution des risques
  - Mesures de sécurité
    - Prévention et détection d'intrusion
  - Plate-formes
    - Intégration SPIAC
  - Plans de secours

- Analyse d’impact métier
- Analyse des risques de continuité
- Plans de continuité informatique

– Analyse des risques

Les éventuels appels d’offres nécessaires pour ces différents projets seront conduits selon les procédures prévues par la loi sur les marchés publics.

8 CONSÉQUENCES DU PROJET DE DÉCRET

8.1 Conséquences sur le budget d'investissement

Ce projet d’investissement est inscrit dans les budgets et plan d’investissement 2013-2015 ; il est référencé dans Procofiev sous le No 600'545. La répartition temporelle proposée dans le tableau ci-dessous sera adaptée lors des processus usuels de révision annuelle de TCA (tranches de crédit annuelles), en fonction de l’évolution de la planification de l’ensemble des projets informatiques.

En francs

Intitulé	Année 2013	Année 2014	Année 2015	Année 2016	Total
a) Transformations immobilières : dépenses brutes					
a) Transformations immobilières: recettes de tiers					
a) Transformations immobilières : dépenses nettes à charge de l'Etat					
b) Informatique : dépenses brutes	3'900’000	4'000’000	731’500		8'631’500
b) Informatique : recettes de tiers					
b) Informatique : dépenses nettes à charge de l'Etat	3'900’000	4'000’000	731’500		8'631’500
c) Investissement total : dépenses brutes	3'900’000	4'000’000	731’500		8'631’500
c) Investissement total : recettes de tiers					
c) Investissement total : dépenses nettes à la charge de l'Etat	3'900’000	4'000’000	731’500		**8'631’500**

L'objet Procofiev 600'545 a été introduit au budget d'investissement 2013 et plan 2014-2017 avec les montants suivants :

Année 2013 CHF 2'100'000.-

Année 2014 CHF 2'000'000.-

Année 2015 CHF 2'000'000.-

Année 2016 CHF 0.-

Année 2017 CHF 0.-

Le montant prévu pour 2013 a été revu à la baisse lors de la révision de janvier 2013 et se situe à CHF 1'479'000.-.

8.2 Amortissement annuel

Cet investissement sera amorti en 5 ans. Cela représente un montant de CHF1'726’300.- par an dès 2014, conformément à l’art. 54 al. 3 de la loi sur les finances.

8.3 Charges d'intérêt

La charge d’intérêt que représente cet investissement, calculée au taux de 5%, est de CHF237’366.25 par année. En chiffres arrondis à la centaine supérieure, cela représente un montant annuel de CHF 237’400.-. Cette charge débutera en 2014.

8.4 Conséquences sur l'effectif du personnel

Pour cette phase, en plus des ressources prévues dans la rubrique ‘ *prestations’*, des ressources internes participeront aux projets. La DSI cherchera à optimiser l’affectation des effectifs aux activités pour couvrir les besoins, notamment en optimisant les processus et en dégageant des économies en internalisant des ressources externes financées par le budget de fonctionnement.

Dans le cadre des projets financés par le présent EMPD, la DSI se réserve la possibilité de faire appel à des ressources complémentaires engagées sous forme de contrats de location de service (LSE) ou de mandataires externes, selon les opportunités et les compétences recherchées, tout en privilégiant les solutions les plus avantageuses.

8.5 Autres conséquences sur le budget de fonctionnement

Dans le tableau qui suit, sont répartis les coûts de fonctionnement nets supplémentaires annuels des différents projets liés au présent EMPD dès 2014 ceci pour un montant de CHF1'087’000.-.

Pour 2013, les projets commençant courant de l’année, les coûts seront inférieurs et vont s’élever à CHF 535'000.-.

En francs

Projets et sous-projets	Exploitation	Logiciel	Total
Diminution des risques			
→ *Mesures de sécurité*			
→ Prévention et détection d'intrusion	50'000	32'000	82'000
→ Sécurité des données	20'000	60'000	80'000
→ *Plate-formes*			
→ Intégration SPIAC		10'000	10'000
→ Remplacement de composants et intégration GDIA	360'000	534'000*	894'000
→ Intégration Cyberadministration			0
→ Cloisonnement de l'infrastructure	105'000	135'000	240'000
→ *Plans de secours*			
→ Premières mesures de continuité	30'000	30'000	60'000
→ Analyse d'impact métier			0
→ Analyse des risques de continuité			0
→ Plans de continuité des activités			0
SMSI			
→ *Processus composant le SMSI*			0
→ *Centre de sécurité opérationnel*	30'000	30'000	60'000
→ *Gestion des incidents de sécurité*			
→ SIEM	40'000	40'000	80'000
→ Outils de réponse aux incidents de sécurité	10'000	40'000	50'000
Analyse des risques			0
Formation			0
Total intermédiaire du budget de fonctionnement	645'000	911'000	1'556'000
→ Remplacement de composants et intégration GDIA**	-385'000	-84'000	-469'000
Total du budget de fonctionnement	260'000	827'000	1'087'000

*) Ce montant comprend la couverture pour le support de la plate-forme et des licences

**) Pour GDIA, l'arrêt des anciens composants remplacés implique une diminution des charges du budget de fonctionnement.

Ces montants font partie de la dotation financière prévue dans le cadre du budget de fonctionnement 2013 (montants budgétés pour la gestion de la sécurité des SI, conformément au plan directeur cantonal des SI adopté par le Conseil d'Etat). En ce qui concerne les impacts financiers à compter de l'année 2014, ils seront totalement financés par le budget de la DSI, grâce à une proposition d'optimisation des ressources de la DSI (internalisation de ressources externes inscrites au budget de fonctionnement).

8.6 Conséquences sur les communes

Les fonctionnalités utilisées par les communes, notamment en ce qui concerne les échanges électroniques (site et portail Internet / accès aux registres des personnes physiques), seront plus sécurisées.

8.7 Conséquences sur l'environnement, le développement durable et la consommation d'énergie.

Néant.

8.8 Programme de législature et PDCn (conformité, mise en œuvre, autres incidences)

Le présent EMPD répond aux orientations stratégiques du Conseil d'Etat de novembre 2008 et à la PGSSI-VD validée par le Conseil d'Etat en juin 2011. Il est aussi conforme au plan directeur cantonal des SI 2009-2013, adopté par le Conseil d'Etat le 25 novembre 2009 et dont certains objectifs ont un effet direct sur l'ouverture au grand public des systèmes d'information étatiques. Ceux-ci sont:

· Le développement et l'ouverture des registres cantonaux

· La mise en œuvre du guichet électronique

· La consolidation des plate-formes communes prioritaires, dont la gestion des identités et des accès (GDIA)

Afin d'éviter que ces derniers projets n'induisent une augmentation dangereuse des risques, une sécurisation adéquate doit être effectuée de manière proactive, ce qui justifie la demande de moyens de sécurité figurant dans cet EMPD.

8.9 Loi sur les subventions (application, conformité) et conséquences fiscales TVA 6

Néant

8.10 Conformité de l'application de l'article 163 Cst-VD

Conformément à l'article 163, 2ème alinéa Cst-VD, lorsqu'il présente un projet de décret entraînant des charges nouvelles, le Conseil d'Etat est tenu de proposer des mesures compensatoires ou fiscales simultanées d'un montant correspondant. Les charges nouvelles sont définies par opposition aux charges dites "liées", soustraites à l'obligation citée. Une charge est liée lorsqu'elle est imposée par une disposition légale en vigueur ou par l'exécution d'une tâche publique, de sorte que l'autorité de décision n'a aucune marge de manœuvre quant à son principe, à son ampleur et au moment où elle doit être engagée (v. art. 7, al. 2 de la Loi sur les finances).

Le présent objet a pour but de permettre à la DSI, créée en 2006, de disposer de moyens minimaux indispensables pour continuer à remplir ses missions, telles que confirmées dans le règlement de l'informatique cantonale adopté par le Conseil d'Etat en janvier 2009.

Une des missions essentielles consiste à assurer la sécurité globale et cohérente des moyens informatiques et de télécommunications indispensables au bon fonctionnement de l'Administration : ceci est en lien direct avec tous les projets et sous-projets proposés dans cet EMPD.

L'ouverture aux citoyens des prestations informatiques de l'Etat oblige la DSI à mettre en place un système de sécurité maîtrisé assurant la continuité nécessaire au fonctionnement quotidien de l'informatique cantonale et de l'ACV, donc à l'exercice des tâches publiques de l'Etat. Les dépenses correspondantes peuvent donc être considérées comme liées dans leur principe.

La quotité de la dépense ne vise qu'au minimum nécessaire à l'accomplissement des missions susmentionnées. Elle doit être par conséquent considérée comme liée.

Quant au moment de la dépense, la dotation de la DSI de moyens et d'outils essentiels à sa mission pour assurer la sécurité informatique avant l'ouverture à la cyberadministration relève de l'urgence et

répond à la volonté du Conseil d'Etat et du Grand Conseil.

En conclusion, les demandes de ressources financières dans cet EMPD doivent être considérées comme des dépenses liées.

A noter que les coûts de fonctionnement (maintenance, exploitation) induits par les projets et sous-projets présentés vont devoir s'inscrire dans le futur budget 2013 de la DSI. Les investissements effectués contribueront à une maîtrise de la sécurité et, grâce à la gestion des incidents de sécurité, à éviter une potentielle perte d'image, une éventuelle violation de la Loi sur la protection des données et des arrêts plus ou moins prolongés de l'opérationnel.

8.11 Découpage territorial (conformité à DecTer)

Néant.

8.12 Incidences informatiques

Néant.

8.13 RPT (conformité, mise en oeuvre, autres incidences).

Néant.

8.14 Simplifications administratives.

Néant.

8.15 Récapitulation des conséquences du projet sur le budget de fonctionnement.

En Francs. Objet No 600'545.

Intitulé	2013	2014	2015	2016	Total
Personnel supplémentaire (ETP)					0
Frais d'exploitation supplémentaires	535'000	1'556'000	1'556'000	1'556'000	5'203'000
Charge d'intérêt		237'400	237'400	237'400	712'200
Amortissement		1726'300	1726'300	1726'300	5'178'900
Prise en charge du service de la dette					0
Autres charges supplémentaires					0
Total augmentation des charges	535'000	3'519'700	3'519'700	3'519'700	**11'094'100**
Diminution de charges [1] (GDIA) Diminution de charges [2] (internalisation RH externes)		469'000 1'087'000	469'000 1'087'000	469'000 1'087'000	1'407'000 3'261'000
Revenus supplémentaires					0
Total net	535'000	1963'700	1963'700	1963'700	**6'426'100**

Pour 2013 le montant indiqué [1] est inclus dans le budget de fonctionnement de la DSI. Le montant récurrent de CHF 469'000 est compensé durant les années suivantes grâce à la réutilisation des ressources affectées au fonctionnement des composants remplacés (GDIA).

La diminution des charges restante [2] dès 2014 (1'087'000 CHF/an) sera réalisée grâce à une optimisation et un redéploiement des ressources financées par le budget de fonctionnement de la DSI (internalisation de ressources externes de type LSE). En dehors de cette optimisation financière, cette

dernière mesure contribue à la réduction de risques induits par une externalisation excessive de tâches pérennes notamment sur les systèmes et applications critiques.

9 CONCLUSION

Vu ce qui précède, le Conseil d'Etat a l'honneur de proposer au Grand Conseil d'adopter le projet de décret ci-après :

PROJET DE DÉCRET
accordant au Conseil d'Etat un crédit d'investissement de CHF 8'631'500 destiné à financer la mise en place de mesures de diminution du risque et du pilotage de la sécurité des systèmes d'information au sein de la DSI

du 17 avril 2013

LE GRAND CONSEIL DU CANTON DE VAUD

vu le projet de décret présenté par le Conseil d'Etat

décrète

Art. 1

[1] Un crédit d'investissement de CHF **8'631'500** est accordé au Conseil d'Etat pour financer la mise en place de mesures de diminution du risque et du pilotage de la sécurité des systèmes d'information au sein de la DSI

Art. 2

[1] Ce montant sera prélevé sur le compte *Dépenses d'investissement* et amorti en 5 ans.

Art. 3

[1] Le Conseil d'Etat est chargé de l'exécution du présent décret. Il en publiera le texte conformément à l'article 84, alinéa 2, lettre b) de la Constitution cantonale.

Le présent décret entrera en vigueur dès sa publication.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 17 avril 2013.

Le président :	Le chancelier :
P.-Y. Maillard	*V. Grandjean*