canton de vaud
LIBERTÉ ET PATRIE

EXPOSE DES MOTIFS ET PROJET DE DECRET

accordant au Conseil d'Etat un crédit d'investissement de CHF 9'506'000 pour financer l'étape 2 de la mise en place de mesures de diminution des risques relatifs à la sécurité de l'information et à la cyber-sécurité.

TABLE DES MATIERES

Principales abréviations utilisées :

ACV	Administration cantonale vaudoise
CE	Conseil d'Etat
DSI	Direction des systèmes d'information
EMPD	Exposé des motifs et projet de décret
PGSSI	Politique générale de sécurité des systèmes d'information
SI	Système d'information
SMSI	Système de management de la sécurité de l'information
SOC	Centre opérationnel de sécurité (Security Operations Center)
USSI	Unité de sécurité des systèmes d'information

1. PRESENTATION DU PROJET

1.1 Résumé

1.1.1 Préambule

Notre environnement et notre manière de consommer l'information ne cessent d'évoluer, en quantité mais aussi en mobilité. De plus, l'évolution des cyber-risques nous oblige, quant à elle, a constamment et rapidement devoir adapter notre défense pour protéger au mieux les informations et systèmes de l'Administration cantonale vaudoise (ACV). Pour ce faire, le centre opérationnel de sécurité (abrégé SOC pour Security Operation Center) de la Direction des systèmes d'information (ci-après DSI) est un maillon essentiel de la chaîne de protection s'inscrivant dans une stratégie de défense en profondeur allant jusqu'aux données.

L'ouverture croissante de l'accès des systèmes d'information aux citoyens, via la cyberadministration, fait partie de l'évolution naturelle de notre société dans laquelle l'ACV a décidé de s'inscrire via l'adoption par le Conseil d'Etat (CE) du Plan directeur cantonal des systèmes d'information 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.

En ligne avec ces priorités, le programme de législature 2017-2022 du CE réaffirme ces orientations en souhaitant, en particulier, activement accompagner la transition numérique de l'État (mesure 3.4). Dans une logique de transparence et d'ouverture (logique progressive d'Open Government Data), de protection des données personnelles et de maîtrise des coûts, ce projet doit moderniser et gérer de manière proactive les applications et les infrastructures informatiques pour en renforcer l'agilité et la sécurité. Il souhaite également, dans le cadre de son soutien à l'innovation, en particulier accompagner la transition numérique et le développement de la sécurité économique numérique (mesure 2.3).

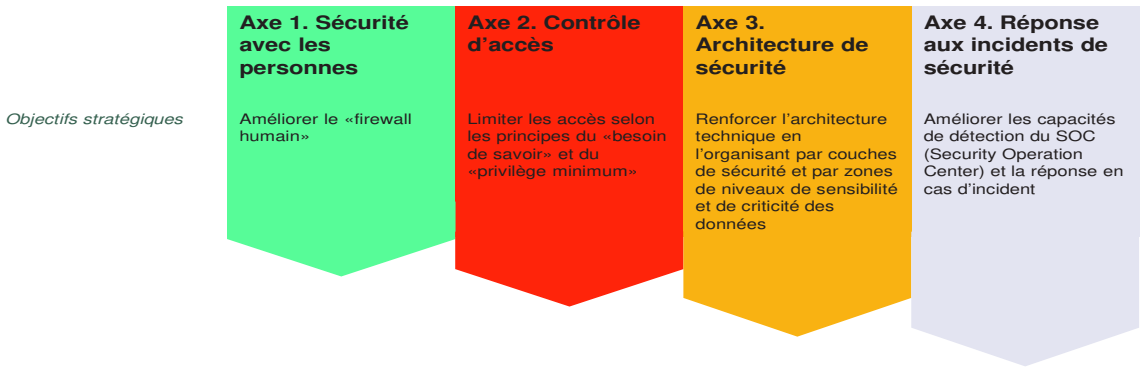
Pour rappel, le Grand Conseil a adopté en novembre 2013 un premier EMPD (réf. EMPD 61) qui a permis de mettre en œuvre les principales améliorations de la sécurité des systèmes d'information suivantes :

- la modernisation partielle de la plateforme de gestion des identités et des accès ;
- l'amélioration de la sécurité avec la mise en place d'un système de management de la sécurité de l'information (SMSI), incluant une analyse de risques complète ;
- la mise en place d'un centre opérationnel de sécurité (SOC) qui traite les incidents de sécurité découlant d'attaques depuis Internet vers l'informatique cantonale ;
- la première phase de cloisonnement macro des infrastructures IT ;
- la mise en place d'une salle informatique de secours en cas de catastrophe avec le redémarrage rapide d'un certain nombre d'applications critique.

1.1.2 Présentation globale du présent projet

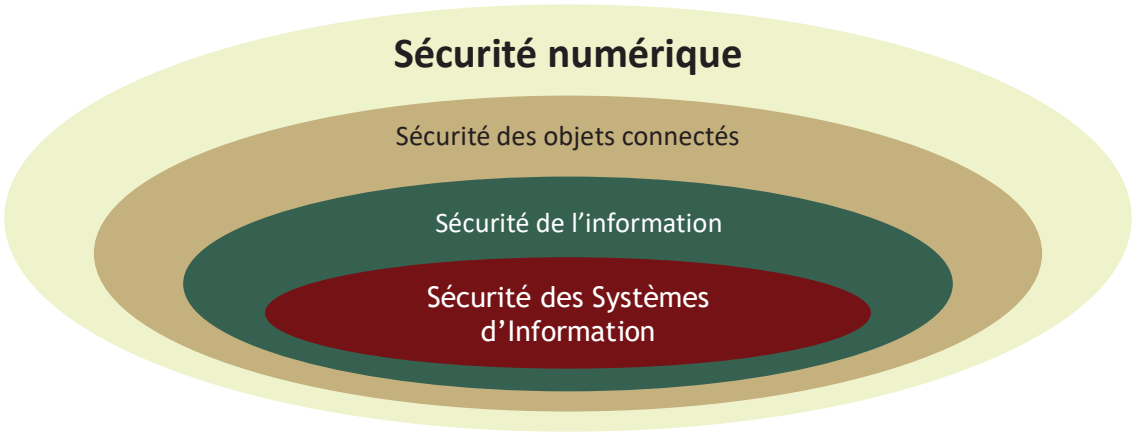
Aujourd'hui, la sécurité de l'information dépasse la dimension technologique des systèmes informatiques et elle doit considérer les processus associés de gestion de la sécurité et surtout intégrer la dimension humaine. Ce n'est que par la bonne combinaison de telles mesures au niveau (i) des personnes, (ii) des processus et (iii) de la technologie que la Direction des systèmes d'information sera en mesure de développer efficacement la sécurité de l'information de l'ACV en se basant sur une gestion des risques pragmatique et alignée sur les meilleures pratiques.

Le présent EMPD s'inscrit dans la continuité des travaux en cours et réalisés ; il va permettre de poursuivre la mise en œuvre des mesures de diminution de risques majeurs selon quatre axes de priorité et d'action :



L'investissement associé à cette 2ème étape de sécurisation du système d'information (ci-après SI) se monte à CHF 9'506'000 et sa réalisation est planifiée sur 5 ans. Les coûts additionnels de fonctionnement annuels mentionnés dans ce document ne sont que ceux qui s'inscrivent dans une augmentation du niveau de sécurité nécessaire à la réduction de risques majeurs et critiques, sans possibilité de compensation des charges par les ressources actuelles de la DSI; ils font donc l'objet d'une solution de financement ad hoc. Il est ainsi prévu que ce projet soit associé à une nouvelle démarche ciblée d'internalisation de ressources externes engagées à la DSI sur des activités pérennes (campagne 2018-2023); ceci dans le but de dégager des économies couvrant notamment les coûts induits par cette nouvelle étape de sécurisation du système d'information cantonal.

Cette étape d'amélioration de la sécurité des SI est un prérequis pour les futures évolutions du SI découlant des programme de législature et plan directeur des SI, notamment en termes de sécurité, en lien avec l'avènement de la société numérique, intégrant en particulier la sécurité des objets connectés.



1.2 Préambule

La Direction des systèmes d'information est en charge de la gestion des systèmes d'information et de télécommunication de l'Administration cantonale vaudoise. 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 (cf. article 6 du RIC).

1.3 But du document

Le présent projet s'inscrit dans la suite annoncée dans l'EMPD (réf. EMPD 61) approuvé en novembre 2013 par le Grand Conseil et couvrant la 1ère étape de sécurisation du SI (Système d'Information).

La suite de ce document s'attache à présenter les travaux et résultats attendus pour cette 2ème étape de sécurisation du SI. Les différentes entités au sein de la DSI se chargeront de mettre en œuvre les projets et mesures de diminution des risques relevant de leurs périmètres respectifs de responsabilité.

1.4 Analyse de la 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'ACV.

Depuis sa création, l'USSI a contribué à la réalisation d'un certain nombre d'actions comme l'élaboration de la Politique générale de sécurité des systèmes d'information (PGSSI) 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 ordinaires limités n'ont permis que d'adresser les fonctions de base de la sécurité sans pouvoir diminuer des risques importants.

Les moyens alloués dans un premier EMPD (réf. EMPD 61), basé sur une pré-analyse des risques, ont permis de mener une analyse des risques complète, de mettre en place un certain nombre de mesures de diminution des risques, de mettre en service un centre de sécurité opérationnel, d'instaurer au sein de la DSI un système de management de la sécurité de l'information (SMSI) et d'équiper un centre informatique de secours en cas de catastrophe pour un nombre limité d'applications critiques.

Aujourd'hui, la DSI doit continuer son effort d'amélioration de la sécurité en se basant sur l'analyse de risques complète actualisée. En effet, celle-ci montre que les systèmes d'information de l'ACV présentent encore des failles dont l'importance ne peut pas être ignorée, en particulier en considérant le déploiement des prestations de cyberadministration.

Les risques majeurs et transversaux identifiés comme devant être diminués par de nouvelles mesures sont :

Risques majeurs	Exemples de types de menaces	Exemples de conséquences négatives
1. Une attaque informatique	▪ Infection majeure par codes malveillants ▪ Intrusion dans le système d'information	▪ Indisponibilité d'applications métiers ; ▪ Données corrompues ; ▪ Données rançonnées ; ▪ Investigation judiciaire ; ▪ Espionnage de l'Etat ; ▪ …
2. Destruction logique	▪ Indisponibilité d'un composant informatique critique provoquée avec l'aide d'accès indus ou par accident	▪ Indisponibilité d'applications métiers ; ▪ Travail en mode dégradé pour des activités critiques ; ▪ Pertes financières ; ▪ Perte de données et de revenus (encaissement par ex.) ; ▪ …

Risques majeurs	Exemples de types de menaces	Exemples de conséquences négatives
3. Destruction physique	▪ Indisponibilité prolongée des systèmes d'information ou destruction d'un actif informatique critique	▪ Indisponibilité d'applications métiers ; ▪ Heures de travail perdues pour les collaborateurs ; ▪ Pertes financières ; ▪ Travail en mode dégradé pour des activités critiques ; ▪ Perte de données ; ▪ …
4. Fuite de données	▪ La perte, le vol ou l'interception de données sensibles ou en masse	▪ Divulgation d'informations confidentielles ; ▪ Vol de données personnelles (réf. Loi sur la protection des données, LPrD) ▪ Espionnage de l'Etat ; ▪ …
5. Fraude	▪ Exploitation d'une vulnérabilité du Système d'Information en vue d'en tirer des avantages	▪ Pertes financières ; ▪ Image détériorée de l'Etat ; ▪ Espionnage ; ▪ …

Comme l'actualité nous le montre et à défaut de pouvoir les supprimer, les impacts de la survenance de tels risques peuvent ainsi conduire à des situations critiques et sensibles pour l'ACV avec des conséquences négatives :

- opérationnelles ;
- financières directes et indirectes (voir exemple du cas d'indisponibilité ci-dessous) ;
- juridiques et réglementaires ;
- en termes d'image et de réputation.

Au vu de la situation décrite plus haut et des risques encourus, il est nécessaire de poursuivre les améliorations de la sécurité de l'information. Face à l'évolution des risques externes et en particulier des cyber-risques, il est nécessaire d'améliorer notre capacité de défense et de réduire globalement les cinq risques majeurs susmentionnés. Il est entendu que la priorité doit être accordée à la continuité des activités critiques de l'Etat. Aujourd'hui, un crash informatique signifierait dans plusieurs services l'arrêt total, pur et simple, de leurs activités.

Les investissements demandés ici s'intègrent dans une logique de mesures globales intégrant les dimensions (i) des personnes et de l'organisation, (ii) des processus et (iii) de la technologie. Sans eux, les projets et améliorations opérationnels réalisés dans les différents domaines sectoriels ne sont pas suffisants pour apporter une amélioration du niveau global de sécurité des SI de l'ACV et de sa capacité à répondre aux nouveaux défis de la sécurité et de la cyber-sécurité.

1.5 Contenu et limites du projet

L'analyse des risques actualisée, comme indiqué dans les sections précédentes, a permis de confirmer des failles de sécurité identifiées auparavant (pré-analyse de risques citée dans l'EMPD 61) et d'en découvrir de nouvelles. Les principaux risques sur les systèmes d'informations liés à ces failles ont ainsi été non seulement identifiés, mais en plus qualifiés et quantifiés. Un certain nombre d'actions pour diminuer ces risques ont été réalisées ou sont en cours de réalisation, grâce à leur prise en compte dans l'EMPD 61 dans le cadre du processus « traitement des risques ».

Dans la continuité de ces actions, ce nouvel EMPD va permettre de mettre en place des mesures de diminution des risques les plus importants non traités à l'étape 1, selon les meilleures pratiques basées sur la norme internationale ISO 27001. Comme mentionné plus haut, il doit également activement participer à la transition numérique de l'État en apportant une attention particulière à la protection des données personnelles tout au long de leur cycle de vie.

Pour rappel, l'approbation par le Conseil d'Etat de la PGSSI-VD en juin 2011 a contribué à renforcer le positionnement de la sécurité comme élément incontournable des systèmes d'information dans la mise en place de la cyberadministration. En effet, l'Administration cantonale propose 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 failles, 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***.

Pour y répondre et gérer adéquatement les risques de sécurité, ce projet a pour objectif de réduire la probabilité et l'impact d'événements pouvant porter atteinte à la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information de l'ACV. En ligne avec les bonnes pratiques actuelles, le projet complète les améliorations lancées avec le premier EMPD selon la vision schématique résumée ci-après :

	Axe 1. Sécurité avec les personnes	**Axe 2. Contrôle d'accès**	**Axe 3. Architecture de sécurité**	**Axe 4. Réponse aux incidents de sécurité**
Principales actions implémentées – ***Etape 1 (EMPD 1 Sécurité)***	▪ Formation e-learning de sécurité	▪ Mise en place d'infrastructures de base pour la gestion des identités et des accès (ACV et cyber)	▪ Identification et classification élémentaire des données de l'ACV ▪ Mise en place d'une architecture de cloisonnement des environnements informatiques	▪ Création et mise en place opérationnelle du SOC (Security Operation Center) ▪ Mise en place du plan de secours IT et prise en compte des besoins de continuité des métiers (**BCM** - Business Continuity Management)
Principales actions proposées à venir – ***Etape 2 (présent EMPD)***	▪ Programme de sensibilisation pour la sécurité des informations de l'ACV et améliorer la résilience face aux cyber-risques ▪ Principe d'accréditations par zone avec e-learning ▪ Meilleur encadrement des prestations externalisées et des fournisseurs	▪ Industrialisation des processus de gestion des accès lors de l'arrivée, de mutation et du départ d'un utilisateur IT ▪ **Gestion et fédération des identités numériques** ▪ Evolution du système de gestion des accès physiques aux **locaux** de l'ACV (SPIAC)	▪ Amélioration de la sécurité des données sources et des applications ▪ Poursuite de la sécurisation des données pour les principaux environnements informatiques et du périmètre de connexion ▪ Amélioration protection antivirus pour l'espace de stockage des données de l'ACV (NAS)	▪ Extension des cas surveillés et réduction du taux de faux positifs ▪ Formalisation et exercice du processus de gestion d'incidents IT / cyber-incidents et de l'escalade en gestion de crises ▪ Poursuite du déploiement BCM dans l'ACV selon stratégie définie

Les 4 axes de travail illustrent le découpage qui va être appliqué pour concrétiser au mieux les actions à entreprendre, contribuant à la sécurisation du SI de manière cohérente, progressive et selon les meilleures pratiques.

La coordination de ces activités est assurée par le Système de management de la DSI intégrant celui de la sécurité de l'information (SMSI).

1.6 Etude d'alternatives de solutions

Comme souligné dans l'EMPD précédent (réf. EMPD 61), la seule alternative de solution possible est de procéder à une « réduction proportionnée des principaux risques identifiés », basée sur l'analyse des risques complète finalisée début 2015.

1.7 Solution proposée

La solution de diminution des risques proposée se décompose en synthèse de la manière suivante :

	Axe 1. Sécurité avec les personnes	Axe 2. Contrôle d'accès	Axe 3. Architecture de sécurité	Axe 4. Réponse aux incidents de sécurité
Objectifs stratégiques	Améliorer le «firewall humain»	Limiter les accès selon les principes du «besoin de savoir» et du «privilège minimum»	Renforcer l'architecture technique en l'organisant par couches de sécurité et par zones de niveaux de sensibilité et de criticité des données	Améliorer les capacités de détection du SOC (Security Operation Center) et la réponse en cas d'incidents de sécurité
Principales actions proposées à venir – ***Etape 2 EMPD Sécurité***	▪ Campagne annuelle de sensibilisation pour la sécurité des informations de l'ACV et améliorer la résilience face aux cyber-risques ▪ Principe d'accréditations par zone avec e-learning ▪ Meilleur encadrement des prestations externalisées et des fournisseurs	▪ Industrialisation des processus de gestion des accès lors de l'arrivée, de mutation et du départ d'un utilisateur IT ▪ **Gestion et fédération** des identités numériques ▪ Evolution du système de gestion des accès physiques **aux locaux de l'ACV** (SPIAC)	▪ Amélioration de la sécurité des données sources et des applications ▪ Poursuite de la sécurisation des données pour les principaux environnements informatiques et du périmètre de connexion ▪ Amélioration protection antivirus pour l'espace de stockage des données de l'ACV (NAS)	▪ Extension des cas surveillés et réduction du taux de faux positifs ▪ Formalisation et exercice du processus de gestion d'incidents IT / cyber-incidents et de l'escalade en gestion de crises ▪ Poursuite de la mise en place du plan de secours IT et prise en compte des besoins de continuité des métiers de l'ACV (Business Continuity Management)
Commentaires	Concerne les 3 principales populations: • Les utilisateurs ACV • Les fournisseurs • Les utilisateurs avec accès privilégiés (cas des administrateurs IT principalement à la DSI)		Concerne les 4 couches principales du système informatique: • Réseau • Systèmes d'exploitation • Bases de données et couches intermédiaires (middleware) • Application	Aujourd'hui, il est impossible de tout prévenir. En conséquence, il est nécessaire d'améliorer les capacité de détection et de réponse en cas d'incident

Le détail des différents projets et de leurs objectifs par axe d'action est précisé au paragraphe suivant.

Un certain nombre d'actions ont été entreprises grâce à l'EMPD 61 et ont été finalisées. D'autres avaient fait l'objet d'un financement partiel couvrant l'étape 1 et, pour pouvoir continuer et être finalisées, nécessitent un financement complémentaire durant l'étape 2. Elles sont récapitulées dans les tableaux ci-dessous.

1.8 Coûts de la solution

Comme présenté dans la section précédente (§1.7 Solution proposée), cet EMPD permet de financer un certain nombre de sous-systèmes qui couvrent le périmètre global des systèmes d'information gérés par la DSI. Par cette approche, les principes de défense proportionnelle et en profondeur s'appliquent.

L'investissement nécessaire se décompose de la manière suivante :

Axe 1 : sécurité avec les personnes		
Actions principales	**Actions détaillées**	**Justification de financement**
1.1 Programme de sensibilisation pour la sécurité des informations de l'ACV et amélioration de la résilience face aux cyber-risques.	Organisation de campagne de formation et de sensibilisation.	La formation de sécurité en ligne effectuée grâce au financement de l'EMPD 61 a permis d'aborder le sujet de la sécurité auprès des utilisateurs de l'ACV et de commencer à les sensibiliser à ce sujet. Cet effort doit non seulement continuer mais doit en plus évoluer en fonction des menaces qui se présentent sous différentes formes au fil du temps. Ceci va demander un effort financier de CHF 150'000.
1.2 Principe d'accréditations et meilleur encadrement des prestations externalisées et des fournisseurs.	Mise en place d'un principe d'accréditation pour les personnes nécessitant des droits d'accès privilégiés (ex : administrateur de bases de données) et amélioration de la sécurité encadrant les	La mise en place des principes d'accréditation et l'industrialisation de la gestion des fournisseurs de la DSI va nécessiter un financement de CHF 150'000.

Axe 1 : sécurité avec les personnes		
Actions principales	**Actions détaillées**	**Justification de financement**
	fournisseurs en termes de formation et de sensibilisation sécurité.	

Axe 2 : contrôle d'accès		
Actions principales	**Actions détaillées**	**Justification de financement**
2.1 Industrialisation des processus de gestion des identités et des accès au sein de l'ACV.	▪ Normalisation et standardisation des processus de gestion des identités et des accès lors de l'arrivée, de mutations et du départ d'un utilisateur IT (internes et externes). ▪ Standardisation et industrialisation de la gestion des identités pour les services de l'ACV.	▪ La normalisation et standardisation des processus de gestion des identités et des accès, qui consiste en la mise en place d'une gouvernance, va nécessiter un besoin de prestations sur 3 ans se montant à CHF 300'000 pour des renforts DSI et CHF 490'000 en services. ▪ La standardisation et l'industrialisation du processus d'identification des collaborateurs de l'ACV va nécessiter un besoin de prestations se montant à CHF 150'000 pour des renforts DSI et CHF 150'000 en services. Pour le matériel, le besoin va s'élever à CHF 150'000.
2.2 Création d'une identité numérique.	▪ Migration de l'outil de gestion des identités vers nouvelle solution IDM pour l'ACV (Identity Management). ▪ Standardisation des méthodes d'authentification et analyse remplacement de la solution d'authentification forte des cartes à grille.	▪ Le remplacement de l'outil de gestion des identités annoncé dans l'EMPD 61 a été effectué. Néanmoins, celui-ci ne tenait pas compte de l'extension nécessaire à la cyberadministration. Cet EMPD permettra de financer cette partie avec un effort en prestations se montant à CHF 350'000 pour des renforts DSI et CHF 1'200'000 en services (environ 2 ETP sur 3 ans). ▪ Standardisation des méthodes d'authentification o L'authentification centralisée sécurisée et l'intégration des applications métiers (ACSIM) vont demander un effort considérable sur une longue période. Cet EMPD va financer le début de ce travail et l'effort pour la période concernée, en prestations est de CHF 100'000 pour des renforts DSI et CHF 260'000 en services. o Pour la fédération des identités, des prestations seront aussi nécessaires dans un premier temps, à hauteur de CHF 200'000 pour des renforts DSI et CHF 600'000 en services. o L'application nécessitant une évolution pour passer au travers de IAM (Identity & Access Management) pour s'identifier nécessite un investissement de CHF 160'000 en licences et CHF 25'000 en prestations.
2.3 Evolution du	▪ Amélioration de la qualité	▪ Des travaux d'amélioration du système actuel

Axe 2 : contrôle d'accès		
Actions principales	**Actions détaillées**	**Justification de financement**
système de gestion des accès physiques (SPIAC pour Sécurité Physique des Installations de l'Administration Cantonale).	de l'existant pour diminuer les pannes.	sur tous les sites installés sont nécessaires afin d'assurer une meilleure qualité de service et permettre de diminuer fortement les coûts liés aux pannes, ce qui sera économiquement avantageux. Ceci va demander un effort de CHF 112'000 en prestations et CHF 48'000 de matériel.

Axe 3 : architecture de sécurité		
Actions principales	**Actions détaillées**	**Justification de financement**
3.1 Amélioration de la sécurité des données de développements et des applications.	▪ Amélioration de la sécurisation des développements et de la protection des codes sources.	▪ L'amélioration de la sécurité des développements par leur industrialisation va nécessiter un investissement de CHF 250'000 en licences et de CHF 475'000 en prestations.
3.2 Sécurisation des données pour les principaux environnements informatiques.	▪ Evolution de la protection périphérique des environnements IT de production ; Pour les environnements hors production (développement, test, validation, …), réduction de la sensibilité des données par mécanismes d'anonymisation, de chiffrement, de pseudonymisation ou de masquage.	▪ La séparation logique des applications en production par domaine métier, étude et réalisation, nécessitera un financement de CHF 300'000 pour des renforts DSI et CHF 460'000 en services. Se rajoutent CHF 30'000 en location de licences pour 2 ans.
3.3 Sécurisation des données stockées.	▪ Meilleure protection contre les codes malveillants de l'espace de stockage des données de l'ACV (NAS).	▪ Avec l'évolution des menaces qui corrompent les fichiers, la protection de l'espace de stockage commun (NAS pour Network Area Storage) doit être améliorée. Ceci implique l'achat d'un produit dont le prix de licence s'élève à CHF 100'000.

Axe 4 : réponse aux incidents de sécurité		
Actions principales	**Actions détaillées**	**Justification de financement**
4.1 Extension des cas surveillés et réduction du taux de faux positifs au SOC.	▪ Extension des cas surveillés et amélioration des scénarios de menace surveillés. ▪ Extension des zones d'analyse sécurisées des codes malveillants. ▪ Approche « Big data » avec des outils spécialisés, de manière à conserver tout le	▪ L'extension du périmètre de protection à tous les systèmes hébergeant des données sensibles nécessitera des prestations de CHF 200'000 pour des renforts DSI et CHF 250'000 en services. Ces prestations comprennent le développement de nouveaux scénarios de détection et l'intégration de nouvelles sources de données afin d'améliorer les capacités de corrélation qui augmentent la pertinence de la surveillance. ▪ Les optimisations nécessaires pour améliorer

Axe 4 : réponse aux incidents de sécurité		
Actions principales	**Actions détaillées**	**Justification de financement**
	trafic réseau et ainsi pouvoir opérer des recherches efficaces lors d'investigations. ▪ Evolution du SIEM (agrégateur d'événements IT) du SOC pour la détection des nouvelles menaces et l'intégration des sources de données du réseau interne. ▪ Amélioration des indicateurs de pilotage. ▪ Création d'une passerelle sécurisée entre les réseaux de l'ACV et du SOC.	l'efficacité et la pertinence des détections et des analyses opérées par le SOC nécessiteront l'acquisition d'outils spécialisés pour des montants de CHF 250'000 de matériel, de CHF 150'000 de licences et des prestations à hauteur de CHF 50'000 pour des renforts DSI et CHF 400'000 en services. ▪ L'évolution du système de détection central des menaces et de collecte des données nécessitera un investissement de CHF 50'000 en licences. ▪ La construction d'indicateurs de sécurité et de tableaux de bord pour obtenir une vision synthétique du niveau de sécurité réel nécessitera un investissement de CHF 50'000 en renforts DSI et CHF 150'000 en services. ▪ La passerelle sécurisée entre les réseaux de l'administration et le SOC nécessitera des prestations pour CHF 300'000.
4.2 Poursuite de la mise en place du plan de secours IT.	▪ Extension du plan de secours informatiques.	▪ Les travaux nécessaires à la mise en place d'une configuration de secours complète nécessitent CHF 20'000 en prestations et un investissement de CHF 912'000 en licences. L'augmentation de périmètre pour avoir un plan de secours complet nécessite un besoin de surface additionnel et un investissement pour le matériel à hauteur de CHF 300'000.

Hors axes : locaux et machines pour personnel projet temporaire		
Actions principales	**Actions détaillées**	**Justification de financement**
Ressources temporelles additionnelles pendant la durée des projets.	▪ Location de locaux pour pouvoir offrir un environnement de travail au personnel externe qui va intervenir dans les projets financés par cet EMPD. ▪ Utilisation des PC et de l'infrastructure de l'ACV par les prestataires de service qui vont intervenir dans les projets financés par cet EMPD.	▪ Sur les 5'514 jours*homme de renforts DSI et « Autres Biens et Services », il y en a 5'150 qui sont pris en compte et qui auront besoin de bureaux et de machines étatiques. Ceci se traduit en 23,5 ETP sur un an, ce qui correspond à environ 8 ETP sur trois ans. Le coût annuel par ETP se comptabilise en CHF 6'630 par an pour les locaux et CHF 2'500 pour le poste de travail avec toute l'infrastructure sous-jacente. Le coût total de ceci s'élève à CHF 214'000.

Coûts d'investissement *- Montants financiers totaux, en CHF*

Montants financiers en CHF

Investissements	Renforts DSI j*h	Renforts DSI CHF	Autres biens et services	Logiciels et Applications	Matériel hors CI*	Total hors CI*	Matériel CI*
AXE 1 : Sécurité avec les personnes - Améliorer le "firewall humain"							
1.1 Sensibilisation	80	100'000	50'000			150'000	
1.2 Encadrement prestations externes	120	150'000				150'000	
AXE 2 : Contrôle d'accès - Limiter les accès selon les principes du "besoin de savoir" et du "privilège minimum"							
2.1.1 Standardisation IAM	240	300'000	490'000			790'000	
2.1.2 Standardisation cyberadministration	120	150'000	150'000		150'000	450'000	
2.2.1 Brique IDM ACV	280	350'000	1'200'000			1'550'000	60'000
2.2.2 Authentification centralisée (ACSIM)	80	100'000	260'000			360'000	
2.2.3 Fédération des identités	160	200'000	600'000			800'000	
2.2.4 Adaptation applicative			25'000	160'000		185'000	
2.3 Amélioration SPIAC			112'000		48'000	160'000	
AXE 3 : Architecture de sécurité - Renforcer l'architecture technologique en l'organisant par couches de sécurité et par zones de niveau de sensibilité et de criticité des données							
3.1 Sécurité des développements	380	475'000		250'000		725'000	
3.2 Sécurité des données par environnement	240	300'000	460'000	30'000		790'000	
3.3 Sécurisation des données stockées				100'000		100'000	
AXE 4 - Incidents de sécurité - Améliorer les capacités de détection du SOC et la réponse en cas d'incidents de sécurité							
4.1.1 Extension scénarios de menaces	160	200'000	250'000			450'000	400'000
4.1.2 Optimisation détections SOC	40	50'000	400'000	150'000	250'000	850'000	
4.1.3 Evolution du SIEM du SOC				50'000		50'000	200'000
4.1.4 Construction indicateurs sécurité	40	50'000	150'000			200'000	
4.1.5 Passerelle sécurisée			300'000			300'000	
4.2.1 DRP	16	20'000		912'000		932'000	650'000
4.2.2 DRP salle 2					300'000	300'000	
Hors AXES - Locaux et machines pour personnel projet temporaire							
Plateforme projets			214'000			214'000	
Totaux	***1'956***	***2'445'000***	***4'661'000***	***1'652'000***	***748'000***	***9'506'000***	***1'310'000***

Fig. 1 - Tableau des coûts complets d'investissement

**) CI : Crédit d'inventaire pour l'acquisition du matériel informatique et de télécommunication*

Coûts de fonctionnement *- Montants financiers à terme, en CHF/an*

Fonctionnement, **hors** impacts **RH** internes et hors amortissements et intérêts	Coûts de fonctionnement informatique			Coûts de fonctionnement métier	Total
	Matériel	Logiciels	Prestations		
AXE 1 : Sécurité avec les personnes					
-					0
AXE 2 : contrôle d'accès					
2.1.1 Standardisation IAM	70'000	160'000	130'000		360'000
2.2.1 Brique IDM ACV	95'000	100'000			195'000
2.2.3 Fédération des identités			130'000		130'000
AXE 3 : architecture de sécurité					
3.1 Sécurité des développements		50'000			50'000
3.3 Sécurisation des données stockées		30'000			30'000
AXE 4 : incidents de sécurité					
4.1.1 Extension scénarios de menaces	80'000				80'000
4.1.2 Optimisation détections SOC	50'000	30'000			80'000
4.1.3 Evolution du SIEM du SOC	40'000	10'000			50'000
4.2.1 DRP		182'000	175'000		357'000
4.2.2 DRP salle 2				400'000	400'000
Augmentation de charges, hors impacts RH internes	***335'000***	***562'000***	***435'000***	***400'000***	***1'732'000***

Fig. 2 - Tableau des coûts de fonctionnement

Les coûts additionnels annuels induits de CHF 1'682'000 / an à terme se répartissent en des charges de :

- maintenance du matériel (CHF 335'000 /an pour un investissement figurant au tableau précédent de CHF 748’000 + CHF 1'310'000 = CHF 2'058'000).
- maintenance logicielle (CHF 562’000 /an pour un investissement de CHF 1’652’000 au total, cf. Fig 1). Cette maintenance paraît disproportionnée par rapport à l’investissement, mais ceci est dû au choix économiquement plus avantageux de la solution IAM « open source » qui demande un coût d’investissement initial de prestations et pas de licences, mais implique des coûts annuels de support.
- location et utilisation d’une 2ème salle de secours (à hauteur de CHF 400’000 /an).
- prestations externes pérennes à hauteur de CHF 435’000 /an (maintenance logicielle d’outils de sécurité et support d’experts y relatifs, fournis par des mandataires externes dans le cadre de contrats d’entreprise).
- désengagement de l’ancienne solution IDM remplacée pour CHF 50'000 /an dès 2020 (voir chapitre §3.5). Somme à soustraire au total de CHF 1’732'000.

Ces coûts de fonctionnement annuels sont induits par une augmentation du niveau de sécurité nécessaire à la réduction de risques majeurs et critiques, sans possibilité de compensation des charges par les ressources actuelles de la DSI ; ils font donc l’objet d’une solution de financement ad hoc dès 2019, grâce aux rationalisations internes prévues et aux économies qui seront générées en cas d’autorisation d’une nouvelle démarche ciblée d’internalisation de ressources externes engagées à la DSI sur des activités pérennes (campagne 2018-23). Les explications détaillées sont fournies dans le paragraphe 3.5.

1.9 Justification de la demande de crédit

Le présent EMPD se justifie par la volonté du Conseil d’Etat d’atteindre l’objectif de la mise en place d’une sécurité indispensable et proportionnée du SI, pré-requise pour le déploiement de la cyberadministration.

L’analyse de la situation actuelle montre les conséquences potentiellement néfastes du manque de sécurité. Les exemples ne manquent pas ces dernières années, et des entreprises tout comme des administrations publiques, subissent régulièrement des attaques informatiques ou divulgations de données sensibles qui ont provoqué non seulement une perte d’image considérable, mais aussi des pertes financières très élevées souvent liées à l’impossibilité de fournir les prestations habituelles.

Les estimations montrent que l’investissement pour assurer et maîtriser la sécurité des systèmes d’information est indispensable non seulement pour une question de respect des lois (Loi sur la protection des données) et pour

assurer la disponibilité des prestations de l'ACV aux citoyens, mais aussi pour une question de réputation, de confiance et d'image auprès de la population.

1.10 Calendrier de réalisation et de l'engagement des crédits

Cette planification du projet ci-dessous est indicative. Outre son démarrage dépendant de la date d'acceptation de l'EMPD, des arbitrages pourront avoir lieu de manière agile pour s'adapter aux priorités métiers des services bénéficiaires de l'Etat.

Nom projet	2019				2020				2021				2022				2023			
GDIA - Brique IDM																				
GDIA - Concepts et gouvernance																				
GDIA - Projet ACSIM																				
GDIA - Projet FID																				
GDIA - Appui à la cyberadministration																				
SOC - Extension du périmètre																				
SOC - Optimisation																				
Projet CLIN																				
Projet DRP																				
Pilotage de la sécurité																				
Evolution SPIAC																				
Maturité des processus																				
Développements sécurisés																				
Sécurisation des applications internet																				
Sécurisation des données stockées																				

Ce projet d'investissement est inscrit dans les budgets et plan d'investissement 2019 - 2023; il est référencé dans le SI comptable et financier sous le N° I.000624.01.

La répartition temporelle indiquée dans le tableau ci-dessus sera adaptée lors des processus usuels de révision de TCA (tranches de crédit annuelles), en fonction de l'évolution de la planification de l'ensemble des projets informatiques de l'ACV.

Les plannings des projets présentés et les délais indiqués seront ainsi ajustés aux TCA allouées dans le cadre de ce processus.

2. MODE DE CONDUITE DU PROJET

Pour les différents projets de sécurisation des systèmes d'information 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 parties prenantes concernées 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 (services bénéficiaires, fournisseurs).

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

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

3. CONSEQUENCES DU PROJET DE DECRET

3.1 Conséquences sur le budget d'investissement

L'objet d'investissement est inscrit sous l'EOTP I.000624.01 « Sécurisation du SI – Etape 2 ». Il est prévu au budget 2019 et au plan d'investissement 2020-2023 avec les montants suivants :

(En CHF)

Intitulé	Année 2019	Année 2020	Année 2021	Année 2022	Année 2023
Budget d'investissement 2019 et plan 2020-2023	1'000'000	1'276'000	1'100'000	1'000'000	1'000'000

Fig. 3 - Tableau du budget d'investissement réparti par année

La répartition temporelle indiquée dans le tableau ci-dessous sera adaptée lors des processus usuels de révision de TCA, en fonction de l'évolution de la planification de l'ensemble des projets informatiques de l'ACV.

(En CHF)

Intitulé	Année 2019	Année 2020	Année 2021	Année 2022	Année 2023	Total
Investissement total : dépenses brutes	2'700'000	2'700'000	2'200'000	1'350'000	556'000	9'506'000
Investissement total : recettes de tiers	0	0	0	0	0	0
Investissement total : dépenses nettes à la charge de l'Etat	**2'700'000**	**2'700'000**	**2'200'000**	**1'350'000**	**556'000**	**9'506'000**

Les plannings des projets présentés et les délais indiqués seront ainsi ajustés aux TCA allouées dans le cadre de ce processus.

3.2 Amortissement annuel

L'amortissement est prévu sur 5 ans à raison de CHF 1'901'200 par an dès 2020.

3.3 Charges d'intérêt

La charge annuelle d'intérêt sera de (CHF 9'506'000 x 4% x 0.55) CHF 209'132 arrondi à CHF 209'200 dès 2020.

3.4 Conséquences sur l'effectif du personnel

En vue de la mise en œuvre de l'ensemble des projets retenus pour 2018-2023, le plan directeur cantonal des SI adopté par le CE fin 2018 a inscrit l'objectif général « d'augmenter la capacité de la DSI en termes de ressources pour répondre aux besoins, mais à budget constant. Pour y parvenir, il s'agit de : simplifier les processus internes … Internaliser partiellement et de manière ciblée des renforts externes pérennes … » (cf. § 5.2.5 du plan directeur).

Cet objectif se déclinant aussi sur l'axe de sécurisation prioritaire du SI cantonal, il entraînera un redéploiement de ressources internes dès 2019, estimées à une dizaine de contributeurs aux volets sécuritaires des projets puis des tâches de maintenance et d'exploitation induites.

Cette façon de faire va non seulement contribuer à contenir les coûts d'investissement et de fonctionnement, mais aussi à assurer une plus-value pérenne dans la capitalisation des connaissances du personnel interne de la DSI. Le succès des projets concernés (délais et budget) est dépendant de cette condition.

Dans le cadre des projets financés par le présent EMPD (renforts DSI et « Autres Biens et Services » durant la phase projet), la DSI fera appel à des mandataires externes, selon les opportunités et les compétences recherchées, tout en privilégiant les solutions les plus avantageuses.

3.5 Autres conséquences sur le budget de fonctionnement

Eu égard aux différentes explications présentées dans les chapitres ci-dessus consacrés à la description des solutions, les conséquences de la demande de crédit sont les suivantes (en CHF) :

Intitulé	Année 2019	Année 2020	Année 2021	Année 2022	Année 2023
Frais d'exploitation autres que RH - charges supplémentaires	*721'000*	*1'612'000*	*1'632'000*	*1'732'000*	*1'732'000*
Compensation des charges par le désengagement des solutions remplacées		50'000	50'000	50'000	50'000
Compensation des charges par les économies nettes de l'internalisation partielle de RH externes de la DSI, campagne 2019-23	690'000	1'120'000	1'582'000	1'682'000	1'682'000
Compensation des charges via la rationalisation interne, objectif DSI inscrit dans le plan directeur cantonal des SI 2018-23	31'000	442'000			
Total net	***0***	***0***	***0***	***0***	***0***

Fig. 4 - Tableau des autres coûts de fonctionnement annuels prévus (hors amortissements, intérêts et service de la dette)

Les coûts de fonctionnement annuels estimés ci-dessus (cf. chapitre §1.8) sont induits par une augmentation du niveau de sécurité nécessaire à la réduction de risques majeurs et critiques. La solution de financement proposée passe par une nouvelle démarche ciblée d'internalisation de ressources externes engagées à la DSI sur des activités pérennes ; si elle est autorisée, cette opération dégagera ses pleins effets (économies) en fin de législature, étant donné qu'elle ne peut être que progressive (réalisation par lot entre 2019 et 2022). Le complément de financement en 2019-2020 provient de l'objectif de rationalisation interne que s'est assigné la DSI dans le cadre du plan directeur cantonal des SI 2018-23 en cours de finalisation.

3.6 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 davantage sécurisées.

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

La mise en place d'applications additionnelles, qui implique davantage de serveurs physiques dans le centre de secours, va induire une consommation électrique plus élevée.

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

Néant.

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

Néant.

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

3.10.1 Principe de la dépense

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 proposés dans cet EMPD.
La Jurisprudence du Tribunal fédéral, dans un arrêt de 2001, a souligné que l'informatique est aujourd'hui généralement indispensable à l'Etat pour accomplir les tâches administratives qui lui sont dévolues : "Il est aujourd'hui communément admis que l'Etat recourt à l'informatique pour exécuter les tâches administratives qui lui sont dévolues de par la loi, en raison du gain de temps et en personnel qu'implique une telle solution ; les dépenses consenties à cet effet sont de ce fait absolument nécessaires à l'accomplissement d'une tâche de l'Etat , au sens de la jurisprudence rendue en matière de référendum financier […]. Il en va de même à fortiori des dépenses consacrées à améliorer la sécurité du traitement des données informatiques" (arrêt du TF non publié 1P, 722/2000 du 12 juin 2001 consid.3b).

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.

3.10.2 Quotité de la dépense

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.

La dotation de la DSI de moyens et d'outils essentiels à sa mission pour assurer la sécurité informatique avec l'ouverture à la cyberadministration relève d'un point stratégique et répond à la volonté du Conseil d'Etat et du Grand Conseil exprimée à de multiples reprises, notamment à travers l'adoption des crédits d'investissement liés à la cyberadministration.

3.10.3 Moment de la dépense

La protection des données du citoyen est une priorité. Les rapides évolutions dans le domaine informatique impliquent une adaptation continue pour assurer un certain niveau de sécurité des systèmes d'information. Toute attente diminue la qualité de défense aux attaques, ce qui veut dire que plus on attend le moment de la dépense et plus le risque augmente.

3.10.4 Conclusion

Les demandes de ressources financières dans cet EMPD doivent être considérées comme des dépenses liées.

3.11 Découpage territorial (conformité à DecTer)

Néant.

3.12 Incidences informatiques

La mise en place des mesures de diminution des risques va permettre de filtrer et bloquer le maximum d'attaques qui ciblent l'informatique cantonale, attaques qui sont de plus en plus fréquentes. L'importance de ces mesures

est proportionnelle à la sensibilité des données à protéger tout en tenant compte des effets de rebond (partie moins importante, moins protégée qui, une fois compromise, permet de rebondir sur la partie la plus sensible).

Les projets proposés induisent donc l'adaptation et la sécurisation des infrastructures informatiques, et donc des données qui y sont gérées.

3.13 RPT (conformité, mise en œuvre, autres incidences)

Néant.

3.14 Simplifications administratives

Néant.

3.15 Protection des données

La protection des données fait partie des buts principaux de la sécurité (confidentialité, intégrité et traçabilité). Le but de l'EMPD précédent (réf. EMPD 61) et de cet EMPD est de diminuer les risques de perte de confidentialité des données, de perte d'intégrité des données et de perte de traçabilité des opérations effectuées sur les données.

3.16 Récapitulation des conséquences du projet sur le budget de fonctionnement

Eu égard aux différentes explications présentées dans les chapitres ci-dessus consacrés à la description des solutions et de leurs impacts, les conséquences de la demande de crédit sont les suivantes :

(En CHF)

Intitulé	Année 2019	Année 2020	Année 2021	Année 2022	Année 2023	Total
Personnel supplémentaire (ETP)						
Frais d'exploitation	721'000	1'612'000	1'632'000	1'732'000	1'732'000	7'429'000
Charge d'intérêt		209'200	209'200	209'200	209'200	836'800
Amortissement		1'901'200	1'901'200	1'901'200	1'901'200	7'604'800
Prise en charge du service de la dette						
Total augmentation des charges	**721'000**	**3'722'400**	**3'742'400**	**3'842'400**	**3'842'400**	**15'870'600**
Diminution des charges		50'000	50'000	50'000	50'000	200'000
Revenus supplémentaires						
Compensation des charges par les économies nettes de l'internalisation partielle de RH externes de la DSI, campagne 2019-23	690'000	1'120'000	1'582'000	1'682'000	1'682'000	6'756'000
Compensation des charges via la rationalisation interne, objectif DSI inscrit dans le plan directeur cantonal des SI 2018-23	31'000	442'000				473'000
Total net	**0**	**2'110'400**	**2'110'400**	**2'110'400**	**2'110'400**	**8'441'600**

Fig. 5 - Tableau des coûts de fonctionnement annuels complets prévus

4. 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 9'506'000.- pour financer l'étape 2 de la mise en place de mesures de diminution des risques relatifs à la sécurité de l'information et à la cyber-sécurité
du 5 juin 2019

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 9'506'000.- est accordé au Conseil d'Etat pour financer l'étape 2 de la mise en place de mesures de diminution des risques relatifs à la sécurité de l'information et à la cyber-sécurité.

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.