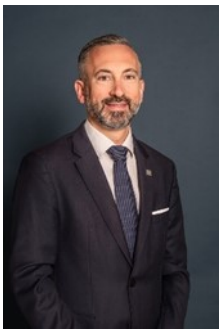
CANTON DU VALAIS
KANTON WALLIS

# Stratégie de cybersécurité du canton du Valais

# *CyberStratVS*

24 décembre 2024



**Frédéric Favre**, Conseiller d'Etat
Président du Groupe de travail

***Ensemble dans un Cyber-Valais sûr et résilient***

La sécurité et la prospérité des Valaisannes et des Valaisans sont au cœur des préoccupations du Conseil d'État. Comme partout ailleurs, le Valais vit une profonde et rapide mutation numérique, une dimension désormais essentielle pour l'État et tout le tissu socio-économique. Face aux cyberdéfis, de nombreuses décisions et mesures ont déjà été prises en Valais ces dernières années, parmi lesquelles la loi sur les bases de données référentielles et la loi sur les services numériques des autorités. En 2022 a également été créée la section cybercriminalité au sein de la police cantonale. L'évolution des risques liés à la mutation numérique de la société exige toutefois que le Valais dispose d'une stratégie de cybersécurité. Comme l'ont abondamment montré les récents cyberincidents dans le monde, seule une politique d'ensemble cohérente parviendra à mieux maîtriser et à diminuer les risques de et dans l'espace numérique afin de tirer pleinement avantage des nombreux progrès qu'il offre.

Tous les acteurs de la société sont exposés aux cyberrisques. Il s'agit d'identifier ces derniers à temps et de s'en prémunir. Les cyberattaques n'arrivent pas qu'aux autres et leurs conséquences peuvent être lourdes. Attendre l'incident, c'est risquer de subir ses effets de plein fouet. Les cyberrisques sont déjà considérés avec sérieux par le Valais et nombre d'organisations et d'entreprises. L'analyse montre toutefois que la maturité générale en matière de cybersécurité et de culture des données et de leurs usages y est insuffisante. Une stratégie et des mesures supplémentaires axées sur l'anticipation sont impératives. Le Conseil d'État entend ainsi limiter les risques liés au numérique et renforcer la sécurité et la résilience des autorités et des acteurs d'importance face aux cyberrisques.

La stratégie de cybersécurité du Conseil d'État s'adresse en priorité aux décideurs de l'administration cantonale, des communes, des institutions parapubliques et des exploitants d'infrastructures critiques afin que s'établisse un continuum cohérent entre ces acteurs. La stratégie crée également les conditions favorables pour que les citoyens et les entreprises assument leurs propres responsabilités en matière de cybersécurité.

La stratégie de cybersécurité du Valais déploiera ses effets dans le temps. Le Conseil d'État est pleinement conscient des efforts et du temps nécessaires pour qu'elle s'établisse comme un réflexe et une culture chez chacun, au même titre que la sécurité routière ou en matière de santé. En conséquence, la stratégie repose sur un suivi de situation et une gouvernance qui, avec toutes les parties prenantes, permettront de mesurer l'efficacité et la cohérence de la stratégie du Valais et de graduellement les renforcer.

**Frédéric Favre**, Conseiller d'Etat
Président du Groupe de travail

# La stratégie en bref

La Stratégie de cybersécurité du Canton du Valais, ou **CyberStratVS**, traduit en actions concrètes la vision du Conseil d'État :

## *Ensemble dans un Cyber-Valais sûr et résilient*

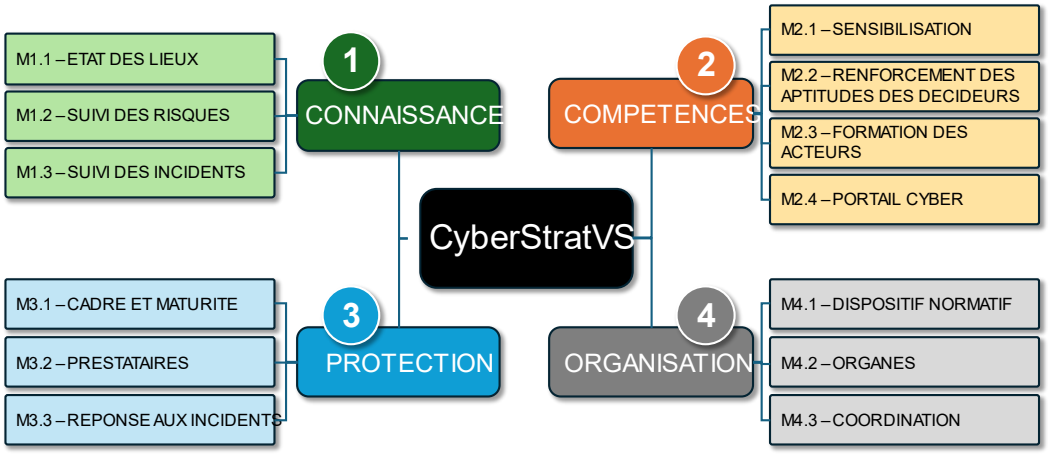
La mutation numérique exige une approche par étapes. Cette stratégie constitue un premier pas afin d'établir une politique cohérente face aux défis posés par les cyberrisques et d'obtenir une connaissance aussi fine que possible de l'écosystème numérique du Valais afin d'améliorer graduellement la pertinence et l'efficacité de son dispositif. La CyberStratVS est un processus s'inscrivant dans la durée et qui doit rester agile pour s'adapter en continu à des défis par nature dynamiques et complexes.

La CyberStratVS n'impose pas de nouvelles obligations. Elle soutient et accompagne – d'abord à l'intention des décideurs, tout en restant accessible à tous les publics intéressés (ci-après : les parties prenantes) – **l'État du Valais**, les **communes**, les **institutions parapubliques** et les **exploitants d'infrastructures critiques** dans la mise en œuvre de bonnes pratiques et en conformité avec les exigences légales. Elle pose les bases d'une collaboration entre les parties prenantes et les invite à l'échange d'information et à la mutualisation de moyens et d'actions chaque fois que cela est possible.

Pour réaliser la vision, **quatre objectifs** ont été définis :

1. Le Valais a une **connaissance** actualisée du niveau de préparation des parties prenantes ;
2. Le Valais dispose des **compétences**, des capacités et des collaborations nécessaires au renforcement de la confiance face aux cyberrisques ;
3. Le Valais assure un niveau de **protection** et de résilience numériques approprié ;
4. Le Valais dispose d'une **organisation** définissant les responsabilités et compétences des parties prenantes face aux cybermenaces.

Ces objectifs sont matérialisés par **13 mesures** et **34 actions**.




Pour assurer la mise en œuvre de la CyberStratVS, deux entités clés ont été définies :

- Niveau stratégique : la haute surveillance de la CyberStratVS est déléguée au **Groupe de coordination cybersécurité VS** qui pourra s'entourer d'un **conseil consultatif cybersécurité** avec notamment des représentants des parties prenantes.
- Niveau opératif : la réalisation concrète de la CyberStratVS est confiée à l'**Entité cybersécurité VS** dont la tâche est de concrétiser la CyberStratVS en étroite collaboration avec les ***référents cyber*** **des parties prenantes**.

Enfin, pour assurer l'exhaustivité des mesures et actions et de les rendre compatibles avec la structure de travail préconisée par la Confédération et d'usage dans l'industrie, la CyberStratVS s'appuie sur les **6 piliers du standard NIST**[1]: gouvernance, identification, protection, détection, réponse et rétablissement.

[1] NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technologie) [https://www.nist.gov/system/files/documents/2022/10/03/NIST_CSF_update_Fact_Sheet.pdf].

CANTON DU VALAIS
KANTON WALLIS

# TABLE DES MATIÈRES

# Portée du document

## Objectif

La stratégie de cybersécurité du Valais vise à fédérer et à coordonner (le mot « **ensemble** » de la vision) les instances valaisannes afin que la société valaisanne, toujours plus numérisée (l'expression « **cyber-Valais** » de la vision) lui garantisse de vivre et de travailler dans un environnement aussi sûr que possible (le mot « **sûr** » de la vision auquel se rattachent les notions de confiance et de souveraineté) et qui, en cas d'incident soit capable de continuer à fonctionner et de se rétablir rapidement (la notion de « **résilience** » dans la vision).

## Public cible

Le périmètre de cette stratégie comprend les parties prenantes suivantes :

- l'**État du Valais**,
- les **communes**,
- les **institutions parapublics et de droit public,**
- les **exploitants d'infrastructures critiques**[2].

Ces entités doivent garantir que les données et les systèmes qui les traitent, et dont elles ont la charge et la responsabilité, sont protégés et fonctionnels conformément aux bases légales ainsi que dans le respect des tâches, rôles et compétences de chacun. La stratégie établit un continuum avec les prestataires d'importance nationale, les tiers, le grand public et les milieux économiques. Elle évite ainsi que ne se créent des discontinuités profitant aux acteurs de la menace et s'assurent que toutes les parties prenantes de la société valaisanne sont conscientes de leurs risques et responsabilités dans le cyberespace.

## Évolution dans le temps

Les cyberrisques, les services et les technologies évoluent rapidement. Pour s'adapter en continu aux changements, le Conseil d'État met donc en place une structure et une gouvernance qui ont pour mission d'assurer sur le long terme la mise en œuvre de la CyberStratVS avec l'ensemble des parties prenantes. Les progrès seront mesurés au moyen **d'indicateurs de performance** et les résultats atteints contribueront à déterminer quand et comment les mesures devront être adaptées / complétées et quand la stratégie elle-même devra éventuellement être révisée.

## Structure du document

Cette stratégie de cybersécurité comprend quatre chapitres :

[2] En s'appuyant sur la Stratégie nationale de protection des infrastructures critiques de l'Office fédéral de la protection de la population OFPP [https://www.babs.admin.ch/fr/strategie-nationale-de-protection-des-infrastructures-critiques], le périmètre de la CyberStratVS se limite aux infrastructures relevant de la responsabilité des autorités valaisannes.

- le premier expose **les défis** justifiant pourquoi une stratégie cantonale de cybersécurité est impérative;
- le deuxième présente **l'état de la cybersécurité** en Suisse et en Valais, les attentes exprimées par les instances consultées durant l'élaboration de la CyberStratVS ainsi que les enseignements des exercices effectués;
- le troisième présente **la stratégie** elle-même, la vision du Conseil d'État, les objectifs et la répartition des rôles et responsabilités des parties prenantes;
- enfin, le quatrième expose **la manière dont la stratégie sera mise en œuvre**.

Les mesures concrètes sont présentées à l'annexe 1 qui pourra ainsi faire l'objet d'adaptations aux nouvelles situations sans devoir adapter la stratégie elle-même.

# 1. Les défis du numérique

## 1.1. Mutation de la société

Au cours des quatre dernières décennies, les technologies de l'information et de la communication (TIC) ont profondément bouleversé la société. De simples outils, elles sont devenues le moteur d'une mutation sociétale au cours de trois grandes phases. Tout d'abord, les TIC ont permis d'optimiser les processus de travail. Ensuite, elles ont facilité l'interconnexion des objets et des entités. Aujourd'hui, la dépendance de la société aux TIC et aux données – leur carburant – est mondiale et irréversible.

Aucune activité humaine, qu'il s'agisse de santé, d'éducation, d'énergie, de transports ou encore de sécurité publique, ne peut plus se passer de cette couche technologique et de ses services, alors que tous reposent de manière critique sur un approvisionnement énergétique aussi sûr que possible. Le cyberespace ne se réduit pas aux TIC et il convient de prendre en compte une multitude de facteurs tels que les ressources humaines, l'éducation (afin d'atteindre une solide culture des données et de leur usage[3]), les législations, les infrastructures, les ressources naturelles, ou encore les finances, dans une approche systémique et de durabilité.

## 1.2. Menaces et dangers dans l'espace numérique

La maîtrise de l'environnement numérique est un enjeu crucial pour la société, nécessitant un cadre à la fois flexible et clairement défini. Le cyberespace, en raison notamment de sa volatilité, des incertitudes qui lui sont associées et de sa complexité, représente un défi majeur. Certaines de ses dimensions posent déjà des risques ou des menaces concrètes, tandis que d'autres pourraient le devenir si elles ne sont pas gérées de manière proactive. Identifier et comprendre à temps les évolutions afin d'en anticiper les risques est donc impératif.

Avec leur omniprésence et leur complexité croissante, les TIC présentent de nombreuses failles souvent exploitées par des acteurs malveillants. Ceux-ci peuvent être des individus, des organisations ou des États. Si certaines vulnérabilités surviennent par hasard, d'autres sont cependant le résultat d'erreurs de développement, comme ce fut le cas lors de la panne mondiale « crowdstrike » du 19 juillet 2024 causée par une mise à jour défectueuse. Certaines failles sont aussi intentionnellement intégrées à notre insu pour servir des intérêts contraires aux nôtres. Certaines sont également le fait de négligences, un comportement d'ailleurs pénalement répréhensible.

Avec les premiers systèmes informatiques sont apparus des programmes malveillants tels que les virus. Ils ont entraîné l'introduction de mesures de sécurité pour

[3] La littératie des données (ou « culture des données », data literacy en anglais) comprend les compétences permettant de collecter, de gérer, d'évaluer et d'utiliser les données de manière critique et réfléchie dans leur contexte respectif, ceci en respectant les principes d'éthique des données et de la protection des données - https://akademien-schweiz.ch/fr/themen/culture-scientifique/data-literacy-charta. A l'ère du numérique où les données jouent un rôle central dans les entreprises, les gouvernements, et même la vie quotidienne et ou leur confidentialité, intégrité, disponibilité et traçabilité sont sans cesse menacées, la culture des données est désormais une compétence essentielle.

protéger les appareils et terminaux. Plus tard, avec l'hyperconnexion, la sécurité a pris de l'ampleur et s'est déclinée à l'échelle des réseaux et des systèmes. L'ère des données, couplée à une multitude de dépendances, exige désormais que la cybersécurité s'établisse au niveau stratégique et soit gérée de manière systémique et non plus uniquement par des mesures techniques. De nouvelles politiques de sécurité permettant de gérer les enjeux sociétaux posés par la mutation numérique et ses défis sont désormais la norme.

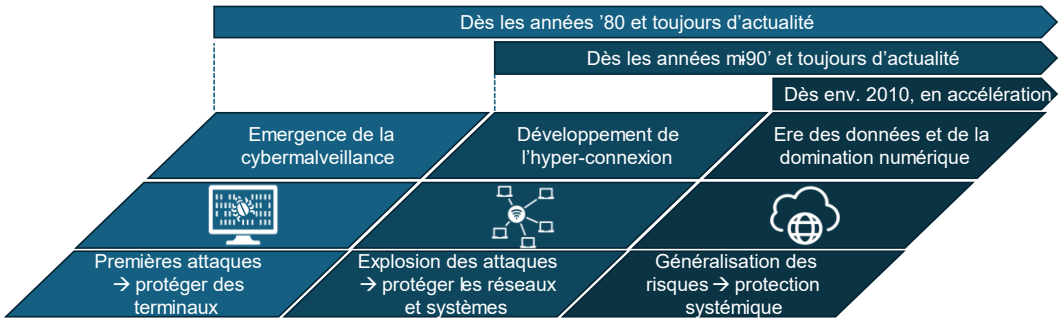



*Figure 1- L'évolution du cyberespace et de la nature de la cybersécurité*

Les acteurs de la menace ont suivi cette évolution. Tout d'abord, il y a eu des **hackers** animés par le jeu, le défi et l'activisme. Sont ensuite apparus les **cybercriminels** ou **cyberpirates** attirés par l'appât du gain, des acteurs malveillants qui ont parfaitement compris la valeur des données, personnelles notamment, et l'usage qu'ils peuvent en faire. Travaillant en bandes organisées professionnelles à l'échelle internationale dans un but d'enrichissement, ces criminels font des ravages.

Selon diverses évaluations, ce fléau coûterait déjà à la société plus de quatre points de PIB, en augmentation constante. Seule une faible partie de ces délits (environ 15%) est portée à la connaissance de la chaîne de poursuite pénale, alors que celle-ci ne parvient à en traiter qu'environ 15%. La troisième catégorie est celle des **cybersoldats** actifs dans le renseignement, le champ politique (par exemple pour influencer les processus démocratiques), ou encore sur le plan militaire comme on l'observe dans le cadre des guerres, notamment entre la Russie et l'Ukraine, ainsi qu'au Proche-Orient.

Le cyberespace est donc un espace de conflictualité à part entière où les belligérants perturbent, espionnent et détruisent les moyens adverses. Les cas récents illustrent par ailleurs combien il est essentiel qu'en matière de cybersécurité le Valais adopte une approche **systémique** et de **maîtrise des chaînes d'approvisionnement**.

Pour les responsables de la cybersécurité dans le canton, la distinction entre les acteurs et leurs intentions – criminelles, d'espionnage, de sabotage, de subversion, ou militaire – importe peu. **Leur mission est d'assurer au quotidien que les données et les processus dont la population et l'économie dépendent soient le**

**mieux possible protégés en matière de confidentialité, d'intégrité, de disponibilité et de traçabilité**[4].

## 1.3. Facteur humain

Malgré les progrès technologiques fulgurants de ces dernières années, l'humain reste au centre de l'écosystème cyber, notamment en tant que cible privilégiée des acteurs malveillants qui profitent de ses faiblesses techniques et psychologiques. Ainsi, une importante partie des attaques découle d'astuces (ingénierie sociale) sans cesse renouvelées. La rapide évolution technologique nécessite donc une adaptation continue des compétences des personnes et des organisations.

La formation continue, que peu d'entreprises et d'institutions parviennent à assurer seules, est ainsi un investissement central pour éviter que n'apparaissent des décrochages et des fossés dans et entre les catégories de populations en raison de différences d'âge (en Suisse, près de 20% de la population a déjà plus de 65 ans), de formation, d'origine, de culture, etc. Cet aspect est d'autant plus important qu'il s'inscrit dans un contexte de pénurie croissante de personnel spécialisé dans les TIC, une évolution qui pèse toujours plus sur la capacité des entités, publiques comme privées, à assurer leurs opérations, leur sécurité et même leurs projets et développements.

Les utilisateurs, décideurs, techniciens, et bien d'autres acteurs, jouent un rôle fondamental dans la cybersécurité qui est une responsabilité partagée, tant dans la sphère professionnelle que personnelle. À l'instar de la santé publique qui ne dépend pas uniquement des médecins et des hôpitaux, ou de la sécurité routière qui ne repose pas uniquement sur la police, la **cybersécurité** n'est pas de la seule responsabilité des informaticiens. Elle **concerne l'ensemble de la société**.

## 1.4. État de la cybercriminalité en Valais

S'agissant des données de la criminalité numérique, la police cantonale suit 33 modes opératoires et 29 types d'infractions au Code pénal répartis en 5 grands domaines : cybercriminalité économique (phishing, hacking, escroquerie, déni de service, etc.), cyberdélits sexuels, cyberatteintes à la réputation et pratiques déloyales, darknet (commerce illégal), autres (fuite de données notamment). En 2023, la police a recensé 1'126 cas, en augmentation par rapport à 2022 de +113% pour la soustraction de données, +117% pour l'accès indu à un système informatique, ou encore +88% pour l'utilisation frauduleuse d'un ordinateur. Les cas de phishing ont quant à eux bondi de 81% et ceux de ransomware de 60%. Il est important de rappeler que ces chiffres ne concernent que les infractions qui sont rapportées aux autorités de poursuite pénale.

[4] Ces quatre principes sont fondamentaux pour établir une stratégie de sécurité globale efficace et sont fréquemment utilisés pour l'évaluation et la conception des mesures de protection des systèmes d'information. Confidentialité : assurer que seules les personnes autorisées aient accès à l'information. Intégrité : garantir que l'information n'est pas altérée ou modifiée de manière non autorisée. Disponibilité : veiller à ce que l'information soit accessible aux utilisateurs autorisés lorsqu'ils en ont besoin. Traçabilité : assurer la capacité d'identifier l'origine d'une information et de toutes les actions qu'elles ont subi afin d'en assurer en particulier l'authenticité.

Ces chiffres inquiétants sont même supérieurs à ceux de l'Office fédéral de la cybersécurité (OFCS) qui, dans son rapport semestriel de mai 2024[5], fait état d'une augmentation en Suisse de 43% des cyberincidents annoncés en 2023 (49'380) par rapport à 2022 (34'527). Pour saisir la gravité de la situation, il convient de prendre en compte que ces chiffres ne représenteraient[6] que le 15% des cas réels. Le nombre effectif pour le Valais aurait ainsi été de près de 7'500 cas en 2023, soit 20 cyberincidents par jour, avec des conséquences économiques et personnelles largement sous-estimées.

## 1.5. Perspectives

Les TIC occupent désormais un rôle central dans la société. Comme constaté dès fin 2022 avec des outils d'IA générative tels que ChatGPT d'OpenAI, Copilot de Microsoft ou Gemini de Google, toujours plus de technologies disruptives émergent. Cette tendance tend à s'accélérer, en particulier dans des domaines tels que les objets connectés, l'intelligence artificielle, l'informatique quantique[7] et les technologies spatiales.

Ce progrès entraîne à son tour de nouveaux risques qu'il faut constamment surveiller et évaluer et que les tensions géopolitiques exacerbent. Le défi principal de toute organisation, particulièrement lorsque les ressources sont limitées, est ainsi de détecter à temps ces bouleversements et leurs répercussions afin de prendre des mesures préventives ou correctrices pour réduire les risques associés. L'anticipation est donc plus que jamais, à tout échelon, un facteur clé. À cet effet une « cartographie » de tous les domaines pertinents, tel que sociétaux, juridiques, financiers, démographiques, environnementaux et énergétiques notamment doit être établie et tenue à jour.

[5] https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2024/ncsc-hjb-2023-2.html

[6] https://www.fedpol.admin.ch/fedpol/fr/home/aktuell/mm.msg-id-101469.html

[7] L'informatique quantique est une technologie émergente qui utilise les principes de la mécanique quantique et permet d'effectuer des calculs complexes avec une rapidité infiniment supérieure aux ordinateurs classiques. Avec ce type de technologie, les acteurs de la menace pourront dans un proche avenir briser tous les modes de chiffrement standards qui protègent la confidentialité des données et des communications.

# 2. État de la cybersécurité en Suisse

## 2.1. Confédération

### 2.1.1. Vision et objectifs

La lutte contre les cyberrisques est un développement récent qui a émergé en 1997 suite à l'exercice de conduite stratégique qui portait sur la « Vulnérabilité de notre société de l'information ». En 2003 a été créée la Centrale d'enregistrement et d'analyse pour la sécurité de l'information (MELANI) et en 2012, la Suisse s'est dotée de sa première Stratégie nationale de protection contre les cyberrisques SNPC à laquelle a succédé en 2023 la ***Cyberstratégie nationale*** CSN[8] actuellement en vigueur :

« *La Suisse saisit les chances offertes par la transformation numérique et engage des mesures de protection pour réduire les cybermenaces et leurs conséquences. Elle compte parmi les leaders mondiaux en matière de connaissances, de formation et d'innovation dans le domaine de la cybersécurité. Dans le contexte des cybermenaces, la capacité d'action et l'intégrité de sa population, de son économie, de ses autorités et des organisations internationales basées sur son territoire sont garanties* ».

### 2.1.2. Dispositif national

Coordonné par l'OFCS, le dispositif national repose sur 3 domaines d'action[9] (figure 2) :

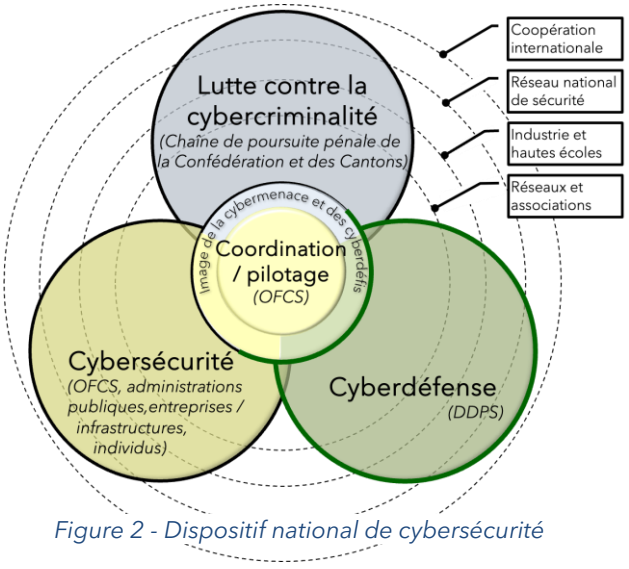



*Figure 2 - Dispositif national de cybersécurité*

- La **cybersécurité** comprend l'ensemble des mesures pour prévenir et gérer les incidents, améliorer la résilience face aux cyberrisques et à développer la coopération.
- La **cyberdéfense** comprend l'ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles; ce domaine inclut des mesures pour identifier les menaces et entraver les attaquants.

[8] https://www.ncsc.admin.ch/ncsc/fr/home/strategie/cyberstrategie-ncs.html

[9] https://www.fedlex.admin.ch/eli/cc/2020/416/fr

- La **poursuite pénale de la cybercriminalité** comprend l'ensemble des mesures de la chaîne de poursuite pénale de la Confédération et des cantons pour lutter contre la cybercriminalité.

Comme illustré ci-dessus, ce dispositif ne saurait fonctionner sans réseaux pour l'appuyer, en particulier le réseau national de sécurité RNS, les collaborations internationales, l'industrie, les milieux académiques ainsi que les réseaux associatifs et professionnels.

### 2.1.3. Moyens principaux[10]

Pour lutter contre les cyberrisques, la Suisse dispose des **instances principales** suivantes au sein du Département de la défense de la protection de la population et des sports (DDPS) :

- le *Secrétariat général du DDPS* (pilotage stratégique, coordination et conseille politique),
- le *Secrétariat d'État à la politique de sécurité* (anticipation et développements en matière de politique de sécurité, sécurité de l'information et contrôles de sécurité relatifs aux personnes et aux entreprises),
- le *Service de renseignement de la Confédération* (suivi de situation en matière de cybermenaces, réponse en cas de cyberattaques contre les infrastructures critiques, lutte contre le cyberespionnage),
- le *Commandement Cyber (*prestations dans le cyberespace et l'espace électromagnétique au profit de l'armée et appuis subsidiaires au profit des partenaires du Réseau national de sécurité),
- l'*Office fédéral de l'armement* / armasuisse (acquisition des connaissances scientifiques et techniques au profit de l'armée et du DDPS, notamment avec le *Cyberdefence Campus*),
- l'*Office fédéral de la protection de la population* (intégration du domaine cyber dans l'analyse nationale des risques de catastrophes et de situations d'urgence et la protection des infrastructures critiques),
- l'*Office fédéral de la cybersécurité* (centre de compétences de la Confédération en matière de gestion des cybermenaces et premier interlocuteur des entreprises, des administrations, des établissements de formation et de la population).

Parmi les **autres acteurs nationaux clés** il convient de citer également :

- le *Réseau national de sécurité* (coordination des cantons en matière cyber), dans le cadre notamment de la Conférence des directrices et directeurs des départements cantonaux de justice et police qui dirige notamment la Prévention Suisse de la Criminalité,
- le Ministère public de la Confédération à l'origine du *Netzwerk digitale Ermittlungsunterstützung Internetkriminalität* ou NEDIK, le réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique sur

[10] https://www.newsd.admin.ch/newsd/message/attachments/89722.pdf

mandat de la Conférence des commandantes et commandants des polices cantonales de Suisse.

### 2.1.4. Bases légales *fédérales* principales

En matière de **droit**, la présente stratégie prend tout particulièrement en compte les textes de loi suivants :

- **Loi sur la sécurité de l'information** (LSI[11]) : cette loi impose nouvellement aux opérateurs d'infrastructures critiques notamment une obligation d'annoncer les cyberincidents et les délais y relatifs.
- **Loi sur la protection des données** (LPD[12]) : cette loi harmonise les pratiques au niveau national et établit une compatibilité juridique de la Suisse avec le Règlement général sur la protection des données RGPD de l'Union européenne.
- **Loi sur le renseignement** (LRens[13]) : en plus des tâches éponymes, cette loi définit notamment l'intervention opérationnelle du Service de renseignement de la Confédération lors de cyberattaques dirigées contre des infrastructures critiques.

## 2.2. Activités dans les cantons

La première version de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) se concentrait sur les actions au niveau de la Confédération. Lors de la révision de 2018, une annexe a assigné aux cantons quatre objectifs : ▸ améliorer les compétences au sein de leurs administrations, ▸ participer au partage des connaissances sur les cybermenaces, ▸ renforcer leur résilience informatique et ▸ contribuer à la création d'une base commune d'échanges d'expériences.

La nouvelle CSN a été validée par les cantons lors de l'assemblée plénière de la Conférence des directrices et directeurs des départements cantonaux de justice et police du 13 avril 2023. Elle est désormais pleinement applicable au niveau cantonal. L'hétérogénéité entre les cantons est importante, mais ils se mettent graduellement en ordre de bataille. Plusieurs cantons disposent désormais d'une stratégie de cybersécurité ou de groupes de travail pour coordonner les principaux acteurs. Divers projets de lois sur la sécurité de l'information et la cybersécurité sont également en cours.

La **Conférence latine des directeurs cantonaux du numérique** (CLDN) a publié en mai 2023 une vision commune sur le thème de la souveraineté numérique[14], notamment sur les plans technique (opportunité d'un Cloud souverain), juridique et socio-économique (définition de la souveraineté numérique) et éthique. La CLDN définit ainsi la souveraineté numérique comme « *la capacité des autorités à maintenir leur autonomie stratégique, soit à pouvoir utiliser et contrôler de*

[11] https://www.fedlex.admin.ch/eli/oc/2022/232/fr

[12] https://www.fedlex.admin.ch/eli/oc/2022/491/fr

[13] https://www.fedlex.admin.ch/eli/oc/2017/494/fr

[14] Les cantons latins veulent renforcer leur action concertée pour la souveraineté numérique

*manière autonome les biens matériels et immatériels et les services numériques qui impactent l'économie, la société et la démocratie* ».

## 2.3. Situation du Valais

### 2.3.1. Échelon cantonal

8ème canton suisse en nombre d'habitants, 3ème en termes de superficie, 12ème en termes de PIB, bilingue, avec une topographie exigeante qui va du Léman aux plus hauts sommets des Alpes, une économie diversifiée allant de l'agriculture de montagne à la haute technologie en passant par le tourisme et l'industrie, pilier national de l'énergie avec 28% de la production hydraulique nationale…, le Valais est un canton complexe. Plus que d'autres, il est aussi confronté aux aléas climatiques et à leurs impacts sur les infrastructures critiques comme lors des intempéries de 2024.

Les cybermenaces font l'objet de nombreuses mesures prises à l'échelle cantonale depuis plusieurs années. En 2019, l'Observatoire cantonal des risques du Canton du Valais (OCRI) reconnaissait déjà l'importance des cyberrisques et le 11 décembre 2024, le Conseil d'État a approuvé la nouvelle stratégie cantonale pour la protection des infrastructures critiques (PIC.VS).

Dès 2022, les mesures du canton en matière de cybersécurité ont été intensifiées et de mieux en mieux coordonnées. Les communes ont été interrogées quant à leurs besoins et attentes. Un soutien forensique subsidiaire en cas d'incident a été mis en place par le canton ainsi que des tests de vulnérabilité. Divers supports d'information ont été adressés aux communes et plusieurs exercices réalisés (CyberREG23, CyberVS24). Le canton a en outre soutenu des solutions concrètes comme la labellisation ou la plateforme de sensibilisation elearningcyber.ch. Le besoin d'harmoniser et de renforcer ces mesures a alors conduit, dès 2023, le Groupe de Travail Cybersécurité VS présidé par le Chef du Département de la sécurité, des institutions et du sport (DSIS) à établir la présente stratégie pour l'ensemble du canton.

En matière de bases légales, le Valais dispose d'ores et déjà de plusieurs lois en rapport direct ou indirect avec la cybersécurité :

- **Loi sur l'information, la protection des données et l'archivage** (LIPDA[15]) : cette loi regroupe des dispositions relatives à l'information du public et l'accès aux documents officiels (transparence), la protection des données personnelles et l'archivage des documents officiels.
- **Loi sur les services numériques des autorités** (LSNA[16]) : cette loi a pour objet de créer les conditions-cadres nécessaires au développement, à l'exploitation, à l'utilisation et au financement des services numériques des autorités.

[15] https://lex.vs.ch/app/fr/texts_of_law/170.2

[16] https://lex.vs.ch/app/fr/texts_of_law/170.8

- **Loi sur la protection de la population et la gestion des situations particulières et extraordinaires** (LPPEx[17]) : cette loi règle la coordination de la gestion et de la protection de la population en situations particulières et extraordinaires, l'organisation des mesures préparatoires et la transition progressive entre les situations ordinaires et critiques.

### 2.3.2. Échelon communal

Le questionnaire aux communes de 2022 – avec une solide participation de 66% - a mis en évidence que seuls 13% des communes disposaient d'un responsable informatique. 55% s'estimaient peu ou mal préparées face aux cyberattaques alors que 80% souhaitaient un soutien cantonal, en particulier lors de cyberattaques. Les récents travaux ont montré un besoin pour des standards minimaux, un soutien dans les relations avec les fournisseurs, dans le domaine de l'assurance, des tests d'intrusion, de la formation et des moyens financiers pour ces mesures. Afin de préciser l'état de situation et aider à la formulation des mesures de la CyberStratVS, un questionnaire articulé au standard NIST a été adressé aux communes en septembre 2024. Le taux de réponse supérieur à 65% illustre à nouveau combien les communes sont préoccupées par la cybersécurité.

- En termes d'**identification** et de gestion des parcs informatiques et des données, certaines questions n'ont reçu que 20% de réponses positives, d'autres 90%. Il apparaît par ailleurs que les communes font souvent simplement confiance à leurs fournisseurs. Il est important ici de rappeler que, même en cas de délégation à des tiers, les communes restent responsables des données et des systèmes qui les hébergent.
- En matière de bonnes pratiques relatives à la **protection**, à l'accès aux données, à la formation du personnel, ou encore aux solutions techniques de sécurité, la situation est également hétérogène ; parfois 30% des communes répondent par l'affirmative, parfois 90%.
- Pour les questions relatives à la capacité des communes de surveiller leur infrastructure et de **détection** des incidents, la fourchette oscille entre 60 et 75%. Seuls 20% des communes s'estiment par ailleurs préparées à la gestion de crise.
- Concernant les questions relatives à la **réponse** aux incidents, les communes s'estiment prêtes dans une fourchette de 30 à 40%. La délégation aux fournisseurs vaut souvent pour une réponse positive.
- 40% des communes estiment être armées en matière de **récupération** après incident, mais seuls 15% disposent d'une procédure d'analyse post-incident montrant là aussi une lacune en gestion de crise.
- En matière de **gouvernance**, seuls 40% des communes annoncent disposer d'une politique de cybersécurité et de rôles définis.

Ces résultats bigarrés, et dans l'ensemble insatisfaisants du **degré de cybermaturité** des communes, montrent l'effort devant être fourni pour les amener à une

[17] https://lex.vs.ch/app/fr/texts_of_law/501.1.

valeur cible satisfaisante. Il faut toutefois relever que les communes s'étant engagées sur le chemin de la labellisation annoncent un degré de préparation en général supérieur aux autres.

Lors des ateliers et échanges bilatéraux, les représentants des communes ont confirmé le faible degré de maturité mis en évidence par le questionnaire. Ces responsables – souvent non spécialisés et de milice – ont unanimement fait part de la **solitude** dont ils souffrent face aux défis et à la complexité de la mutation numérique et des risques y relatifs.

### 2.3.3. Institutions parapubliques et infrastructures critiques cantonales

Le Valais compte un grand nombre d'institutions relevant du droit public ainsi que d'infrastructures critiques soumises à de nombreuses contraintes. Les représentants qui ont contribué à l'élaboration de la CyberStratVS constatent toutefois que le cadre en matière de cybersécurité est insuffisant. Les constats et besoins qu'ils formulent sont comparables à celui des communes, avec des responsables de cybersécurité qui expriment également leur solitude. Ils constatent que seule une fraction des organisations faîtières émet des lignes directrices, impératives ou recommandées selon l'importance des infrastructures critiques concernées.

À partir des énoncés recueillis, on observe que la maturité en cybersécurité de ces institutions et infrastructures n'est pas différente de celle des communes. Pour ces acteurs, la mise en œuvre et le maintien de catalogues complexes de critères de cybersécurité sont un défi. Dans la mesure où la plupart gèrent d'importantes données personnelles, une attention particulière et un soutien sont fortement souhaités.

### 2.3.4. Résumé des besoins

Les exercices d'état-major (voir 2.3.1) ont permis d'identifier d'importants points d'amélioration, en particulier :

- la **communication** (réactive et proactive), la numérisation ayant considérablement transformé ce domaine, accéléré le rythme des crises et modifié le comportement du public ;
- le besoin d'une **cartographie** exhaustive ;
- une **collaboration** efficace des acteurs ;
- et **l'échange** continu d'information entre les parties et sa gestion afin de s'assurer que toutes les informations pertinentes sont identifiées et exploitées ;

Les ateliers et échanges avec les représentants des communes, des institutions et des infrastructures critiques ont quant à eux mis en évidence les besoins et attentes suivants :

- **Gouvernance** – La CyberStratVS doit clarifier les rôles et responsabilités des parties prenantes, privées et publiques. Des référents et points de contact clairs sont réclamés, de même qu'une cartographie exhaustive des points et acteurs significatifs. Une majorité estime qu'en matière de cybersécurité l'autonomie communale doit être relativisée et que pour s'assurer de la mise en œuvre concrète des mesures, divers instruments (procédures, loi, audits,

etc.) sont nécessaires, à l'exemple des nouvelles obligations des énergéticiens ou du domaine des finances étatiques.

- **Information** – Les parties prenantes estiment nécessaire que soit établie une culture cantonale de la cybersécurité. Elles expriment un besoin de soutien pour rendre la cybersécurité accessible auprès de divers publics, en particulier des décideurs. Le partage de la connaissance est de première importance et une veille cantonale devrait la soutenir. Il est attendu la mise en place d'un guichet cantonal unique afin de lutter contre l'éparpillement.
- **Formation** – Les participants aux ateliers ont unanimement reconnu l'importance de l'individu et donc les besoins en termes de formation. Les besoins de compétences en matière de gestion de crise ont été particulièrement relevés.
- **Ressources** – Les parties prenantes rencontrent de fortes difficultés en termes de ressources. Mutualisation, harmonisation, collaboration et synergies devraient être des priorités pour y pallier. Le rôle du canton est central et tous estiment crucial qu'il endosse un rôle renforcé. Il s'agira en outre de vérifier l'opportunité de faciliter l'accès à des prestations particulières comme en matière de SOC (Security Operations Center) ou encore de politique d'achats.
- **Cadre** – Des attentes claires ont été exprimées pour que soit établi un catalogue de lignes directrices. Les participants ont toutefois mis en évidence le danger de la complexité et du risque que chaque étage de responsabilité élève le nombre de prescriptions. Elles ont également insisté sur le temps dont elles ont besoin pour leur montée en puissance. Un consensus se dégage pour que soit promues des labellisations et beaucoup estiment qu'une loi dédiée faciliterait la réalisation des mesures.

# 3. Stratégie

## 3.1. Vision

***Ensemble dans un Cyber-Valais sûr et résilient***

**Le Conseil d'État a pour ambition ….**

Les principes d'action suivants – la doctrine d'action – caractérisent la stratégie valaisanne :

- **Anticiper** – Dans un domaine hautement dynamique, le rythme est crucial. Sur la base d'une connaissance approfondie du terrain, il s'agit d'identifier aussi tôt que possible les nouveaux défis et risques afin de ne pas être pris au dépourvu.
- **Accompagner** – Il s'agit de donner une ligne, de créer des conditions favorables et de n'imposer des mesures particulières que lorsque l'intérêt général est en jeu et la plus-value avérée.
- **Collaborer** – Dans un domaine où personne ne possède la connaissance absolue ni tous les moyens d'action, il s'agit de privilégier une approche commune, de partage d'expérience et de subsidiarité afin d'atteindre et de maintenir un état élevé de maturité à des coûts supportables.

## 3.2. Objectifs

Déduits de l'analyse de la situation et de la vision, **quatre objectifs** ont été formulés. Ils sont accompagnés d'intentions exposant l'état ou l'effet final recherché.

| Objectif | Intention / état final recherché |
|---|---|
| 1. Le Valais a une connaissance actualisée du niveau de préparation des parties prenantes. | Il s'agit de :<br>▪ Disposer d'un inventaire dynamique (à jour) des parties prenantes, de leur niveau de préparation et de leurs interdépendances.<br>▪ Évaluer en continu les risques (menaces et dangers) ainsi que leurs conséquences pour les parties prenantes.<br>▪ Comprendre les défis en lien avec la mutation numérique et être en mesure de les anticiper.<br>▪ Disposer d'une connaissance des incidents ayant touché les parties prenantes dans un but d'amélioration continue. |

| Objectif | Intention / état final recherché |
|---|---|
| 2. Le Valais dispose des compétences, des capacités et | Il s'agit de : |

| Objectif | Intention / état final recherché |
|---|---|
| des collaborations nécessaires au renforcement de la confiance face aux cyberrisques. | ▪ Développer la capacité des décideurs à intégrer et à maîtriser les enjeux et risques du domaine cyber.<br>▪ Doter l'ensemble du personnel des parties prenantes des connaissances essentielles face aux défis et risques du numérique et en matière de littératie des données.<br>▪ Disposer de personnel spécialisé compétent pour affronter les défis et risques du numérique.<br>▪ Permettre aux parties prenantes de bénéficier d'un écosystème collaboratif qui les soutient face aux défis et risques du numérique. |
| 3. Le Valais assure un niveau de protection et de résilience numériques approprié. | Il s'agit de :<br>▪ S'assurer que les parties prenantes ainsi que leurs partenaires et leurs prestataires disposent d'un niveau de protection (technique, organisation, processus) correspondant à l'état de l'art.<br>▪ Être en mesure de détecter à temps les incidents ou tentatives d'attaques contre les infrastructures numériques des parties prenantes.<br>▪ Être en mesure d'affronter de manière flexible (*scalable*) les cybercrises.<br>▪ Assurer la continuité des prestations essentielles des parties prenantes. |
| 4. Le Valais dispose d'une organisation définissant les responsabilités et compétences des parties prenantes face aux cybermenaces. | Il s'agit de :<br>▪ Disposer d'une gouvernance cantonale, dans le cadre des principes de subsidiarité et de bonne collaboration, dans laquelle sont établis des rôles et responsabilités clairs permettant une coordination des parties prenantes entre elles.<br>▪ Disposer d'un cadre formel légitimant les principes et actions visant à assurer un niveau adéquat de cybersécurité à l'échelle du canton.<br>▪ Disposer d'un état de situation continu permettant d'apprécier le suivi de la mise en œuvre de la stratégie et de ses mesures. |

## 3.3. Mesures

La concrétisation de la CyberStratVS revêt aux yeux du Conseil d'État une haute importance afin qu'elle aboutisse à l'effet recherché : faire du Valais un canton aussi sûr que possible face aux nombreux cyberdéfis.

La stratégie donne une direction pour plusieurs années. Elle procure aux parties prenantes une vue d'ensemble de la sécurité dans le canton. Elle leur permet, à leur niveau et dans le cadre de leurs responsabilités, de prendre à temps toute mesure utile pour élever le niveau général de cybermaturité. Elle s'appuie sur une approche de « conduite par objectifs » dans le sens tracé par le Conseil d'État pour le bien commun.

Les conséquences de la vision et des objectifs ont une « durée de vie » plus courte. Elles doivent pouvoir être complétées et corrigées à une fréquence plus élevée sans entraîner de modification de la stratégie. Elles se déclinent en **13 mesures** réparties en **34 actions** mesurables (*cf.* annexe 1). Elles feront l'objet d'un monitoring et d'une révision périodique selon les résultats atteints et l'évolution des technologies et défis.

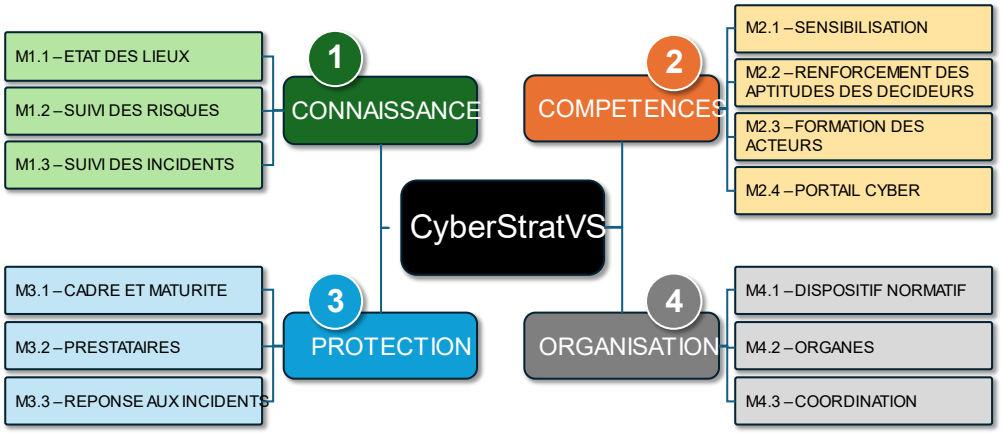



*Figure 3 - Mesures de la CyberStratVS*

## 3.4. Rôles et responsabilités

L'organisation générale et les relations des parties prenantes dans le cadre de la CyberStratVS sont décrites et illustrées ci-après.

- Le Gouvernement délègue la haute surveillance de la CyberStratVS au **Groupe de coordination cybersécurité** (GC cysec), successeur du groupe de travail qui a présidé les travaux jusqu'ici. Au besoin, ce groupe pourra créer un **conseil consultatif cybersécurité** avec notamment des représentants des parties prenantes.
- La mise en œuvre de la CyberStratVS est confiée à l'**Entité cybersécurité VS** (*cf.* mesure M4.2b). Le Conseil d'État décidera ultérieurement de sa structure et de sa dénomination exacte. Cette entité collabore étroitement avec le GC cysec pour la mise en œuvre de la CyberStratVS et notamment ses propositions en matière de développement et de révision conformément aux résultats atteints et l'évolution de la situation et des cyberrisques.

- En cas d'incident touchant une des parties prenantes, l'entité touchée reste, dans tous les cas, responsable de son périmètre. Lorsque ses moyens et ceux de ses soutiens s'avèrent insuffisants, les spécialistes de l'administration cantonale peuvent, s'ils sont disponibles et possèdent les compétences requises, apporter une aide, exclusivement à titre subsidiaire. Lorsque la crise concerne plusieurs entités ou prend une dimension cantonale, l'**Organe cantonal de conduite** (OCC) assure la coordination à l'échelon cantonal, conformément à la LPPEx.

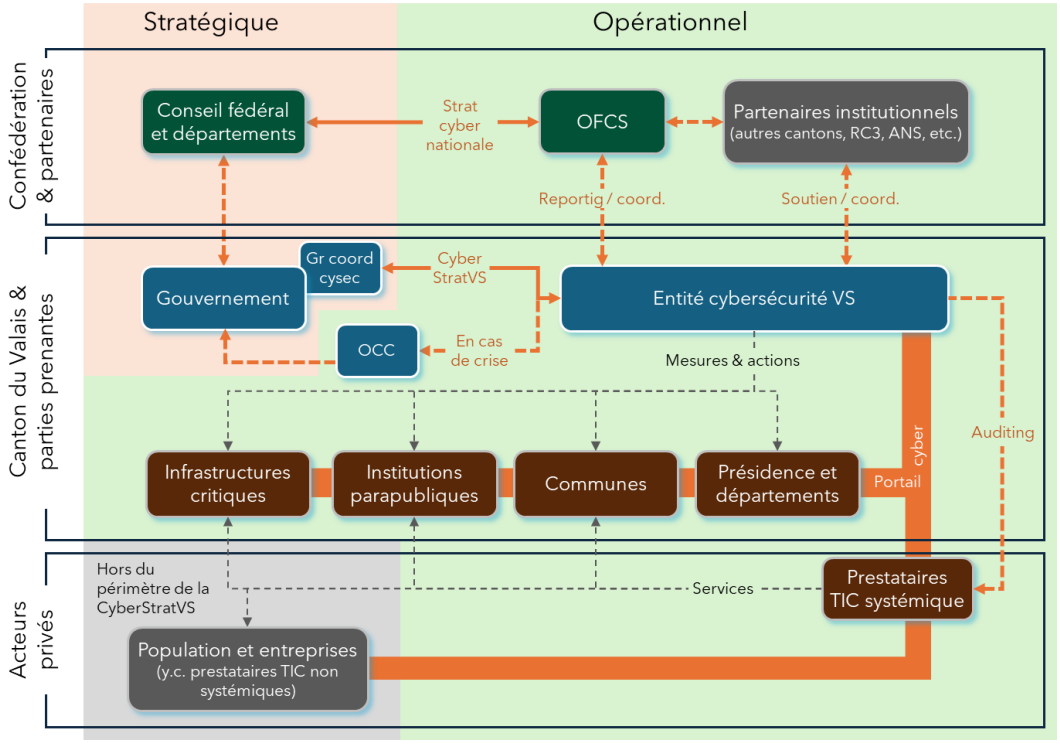



*Figure 4 - Rôles et responsabilités pour la cybersécurité du Valais*

# 4. Mise en œuvre

## 4.1. Mesures de succès (KPI)

Les indicateurs de performance suivants (ou KPI[18]), **exprimés en % du nombre de parties prenantes**[19] seront mesurés. Le suivi de détail sera défini et assuré par l'Entité cybersécurité VS.

a. Désignation des **référents cyber**.

b. Appréciation du **niveau de maturité** (objectif : 2.6 sur 4 selon les Normes minimales pour les TIC[20]).

c. Participation à une **labellisation**.

d. Participation du personnel au **programme de sensibilisation**.

e. Participation des organes dirigeants aux **événements cyber pour décideurs**.

f. Raccordement à un service **SOC**.

g. Conformité des **contrats de prestations**.

h. Intégration des cyberrisques dans les **matrices de gestion des risques**.

i. Préparation à la **gestion de crise**.

j. Réalisation d'**audits** périodiques auprès des prestataires d'importance systémique.

[18] Key Performance Indicator

[19] Sur la base de l'inventaire selon la mesure M1.1a

[20] https://www.bwl.admin.ch/bwl/fr/home/bereiche/ikt/ikt_minimalstandard.html.

## 4.2. Ressources

La concrétisation de la CyberStratVS dépend étroitement des compétences et des ressources allouées. Le GC cysec soumettra annuellement au Gouvernement, sur proposition de l'Entité cybersécurité VS, un budget et une feuille de route adaptés à la situation des cyberrisques et à l'avancement des travaux de la CyberStratVS (voir chi. 4.3).

Le tableau suivant présente les ressources que les parties prenantes sont invitées à **consacrer annuellement** au minimum pour l'augmentation de leur état de préparation face aux cyberrisques.

| | État du Valais | Communes | Institutions parapubliques / de droit public | Exploitants d'infra critiques |
|---|---|---|---|---|
| **Personnel** | ▪ Entités existantes du SCI (cellule cybersécurité), de la police cantonale (section cyber) et d'autres entités (ComSec, etc.).<br>▪ Contributions du SSCM (notamment prot pop).<br>En plus:<br>▪ GC cysec (env. 4 séances de 2h / an pour les membres).<br>▪ Entité cysec VS (2 EPT). | ▪ Référent cyber (charge d'env. 5% pour un employé ou externalisation, soit env. 1 j/mois).[21] | ▪ Référent cyber (charge d'env. 5% pour le responsable cybersécurité, soit, env. 1 j/mois). | ▪ Référent cyber (charge d'env. 5% pour le responsable cybersécurité, soit, env. 1 j/mois). |
| **Budget** | ▪ Matériel et événements de formation et de sensibilisation (100 KCHF).<br>▪ Audits et conseil (70 KCHF).<br>▪ Aides diverses et labellisations (50 KCHF).<br>▪ Capacité CSIRT (selon concept ultérieur – montant additionnel). | ▪ Service SOC (selon stratégie à établir).<br>▪ Exigences minimales et labellisation (selon prix du marché). | ▪ Service SOC (selon stratégie à établir).<br>▪ Exigences minimales et labellisation (selon prix du marché). | ▪ Service SOC (selon prix du marché).<br>▪ Exigences minimales et labellisation (selon prix du marché). |

[21] Il s'agit ici d'un temps estimatif en lien avec le rôle de référent cyber et de coordination qui en découle. Ce temps n'inclut aucunement la gestion globale de la sécurité de la commune, de l'institution ou de l'exploitant d'infrastructure critique.

## 4.3. Feuille de route générale

Les mesures et actions prévues pour concrétiser la CyberStratVS sont toutes importantes, mais leur degré d'urgence est variable. La feuille de route présentée à l'annexe 1 indique le point de départ de chaque action et sera revue annuellement en fonction de l'avancement des travaux.

A des fins d'efficacité et de transparence, chaque mesure fera l'objet d'une planification séparée articulée comme suit : **Priorité** (justifier l'importance et la priorité), **Produit** (définir l'objet et l'effet recherché), **Qualité** (définir le niveau d'ambition), **Intention** (définir le « comment », l'idée de manœuvre pour atteindre le but), **Temps** (définir le point de départ et la durée), **Ressources** (décliner les coûts financiers et en personnel).

# Annexe 1 – Mesures et actions

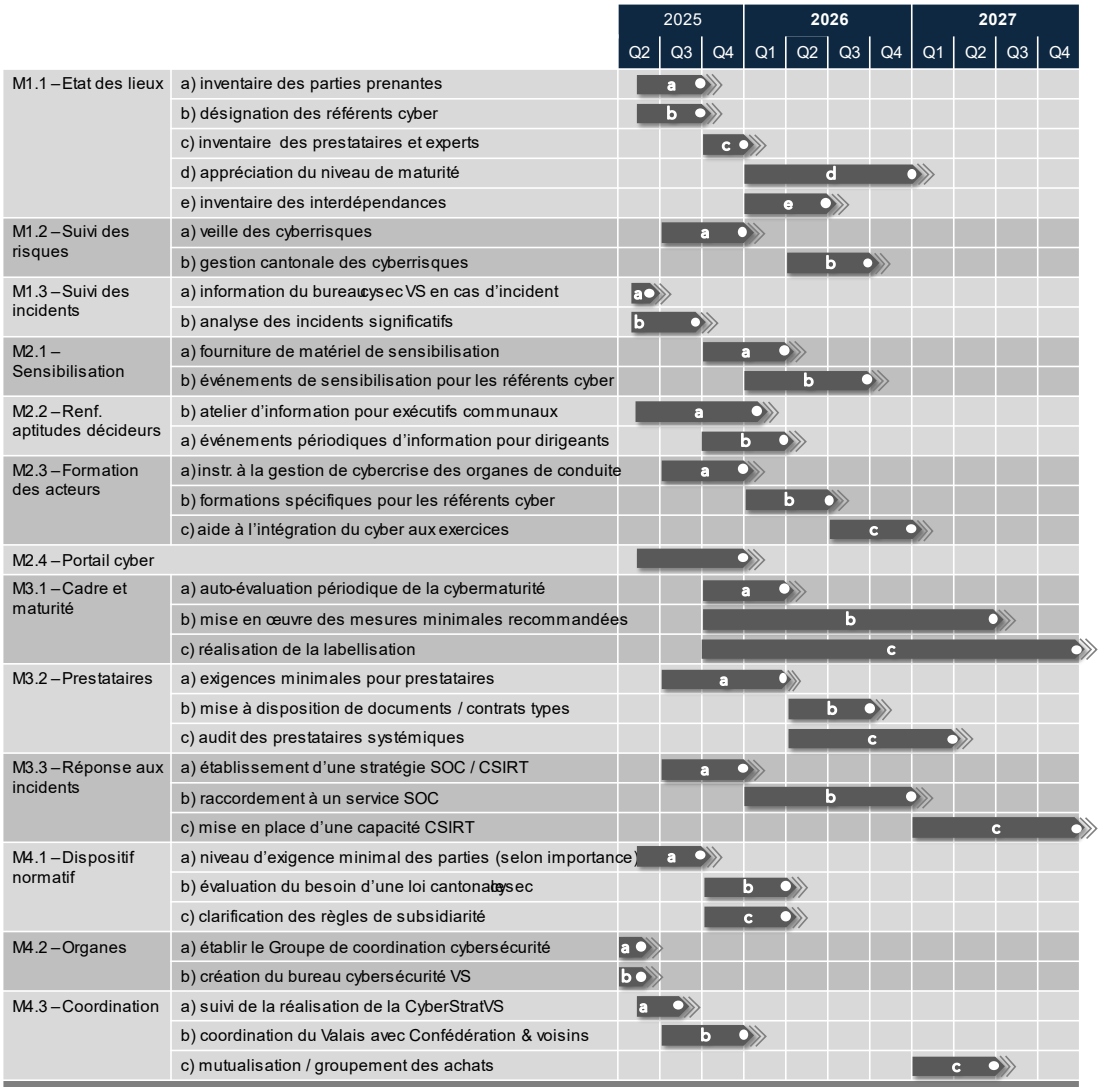
*Légende*

- *Degré de priorité des actions : ❶ = de suite, ❷ = ensuite, ❸ = enfin.*
- *Responsabilité pour la mise en œuvre des actions: VS : État du Valais (Entité cybersécurité VS selon mesure M4.2b) ; tous : toutes les parties prenantes.*
- *Sauf si explicitement spécifié, les actions sont à comprendre dans une approche dynamique et s'inscrivant dans la durée (p.ex. « établir » signifie également « exploiter durablement ».*

| | |
|---|---|
| 1. CONNAISSANCE | **M1.1 – ETAT DES LIEUX**<br>a) Établir l'inventaire des parties prenantes [❶ / VS].<br>b) Désigner des « référents cyber » auprès de chacune des parties prenantes [❶ / tous].<br>c) Établir l'inventaire des prestataires et experts IT actifs en Valais [❷ / VS].<br>d) Établir une appréciation du niveau de maturité de chacune des parties prenantes [❸ / VS].<br>e) Établir l'inventaire des interdépendances [❸ / VS]. |
| | **M1.2 – SUIVI DES RISQUES**<br>a) Conduire une veille des cyberrisques [❶ / VS].<br>b) Établir une gestion cantonale des cyberrisques [❷ / VS]. |
| | **M1.3 – SUIVI DES INCIDENTS**<br>a) S'assurer que l'Entité cybersécurité VS (voir M4.2b) soit informé de tout cyberincident significatif affectant une partie prenante [❶ / VS].<br>b) Analyser tout événement significatif et, si applicable, adresser aux parties prenantes des recommandations [❷ / VS]. |
| 2. COMPETENCES | **M2.1 – SENSIBILISATION**<br>a) Fournir aux parties prenantes [❶ / VS] du matériel de sensibilisation afin qu'elles puissent sensibiliser leur personnel aux cyberrisques [❷ / tous].<br>b) Proposer aux *référents cyber* des parties prenantes des événements de sensibilisation. [❷ / VS]. |
| | **M2.2 – RENFORCEMENT DES APTITUDES DES DECIDEURS**<br>a) Proposer aux membres des exécutifs communaux un atelier d'information cyber à chaque législature [❶ / VS].<br>b) Proposer aux dirigeants des parties prenantes des événements périodiques d'information [❶ / VS]. |
| | **M2.3 – FORMATION DES ACTEURS** |

| | |
|---|---|
| | a) Instruire le personnel des différents organes de conduite / états-majors de crise des parties prenantes aux procédures et à la gestion en cas de cyberincident [❷ / tous].<br>b) Proposer aux *référents cyber* des parties prenantes des formations spécifiques [❷/ VS].<br>c) Assister les organes de conduite / états-majors de crise des parties prenantes pour intégrer le thème cyber dans les exercices [❸ / VS]. |
| | **M2.4 – PORTAIL CYBER**<br>Mettre à disposition des parties prenantes les contenus suivants (liste non exhaustive et évolutive) [❶ / VS] :<br>• la CyberStratVS et sa réalisation ;<br>• toute information, matériel et offre de sensibilisation / formation sur les cyberrisques ;<br>• toute information sur les instances en charge de la cybersécurité et les procédures en cas d'incident ;<br>• toute information sur les critères minimaux à atteindre par les parties prenantes en matière de cybersécurité ;<br>• toute documentation utile sur les bases légales, normes, labels, ainsi que sur les outils d'auto-évaluation. |
| 3. PROTECTION | **M3.1 – CADRE ET MATURITE**<br>a) Réalisation périodique par les parties prenantes d'une auto-évaluation de leur cybermaturité [❶ / tous].<br>b) Mise en œuvre par les parties prenantes des mesures minimales (voir M4.1) recommandées [❷ / tous].<br>c) Mise en place par les parties prenantes d'une labellisation (selon recommandation du canton ou équivalent) [❸ / tous]. |
| | **M3.2 – PRESTATAIRES**<br>a) Fixer des exigences minimales pour les prestataires actifs en Valais en tant qu'aide à la décision des parties prenantes pour l'attribution de mandats [❶ / tous].<br>b) Mettre à disposition des parties prenantes des contrats types / parties de contrat types pour les prestations TIC [❶ / tous].<br>a) Soumettre les prestataires IT revêtant un caractère systémique à un audit régulier [❷ / VS]. |
| | **M3.3 – REPONSE AUX INCIDENTS**<br>a) Établir une stratégie SOC et CSIRT cantonale [❶ / VS]. |

| | |
|---|---|
| | b) Raccorder chaque partie prenante à un SOC [❸ / tous].<br>c) Mettre en place une capacité d'intervention CSIRT (technique, droit, conduite, etc.) en cas de cyberincident [❸ / tous]. |
| 4. ORGANISATION | **M4.1 – DISPOSITIF NORMATIF**<br>a) Définir le niveau d'exigence minimal de cybersécurité pour les parties prenantes selon leur importance [❶ / VS].<br>b) Évaluer l'opportunité de disposer d'une loi cantonale pour la cybersécurité [❷ / VS].<br>c) Développer des règles de subsidiarité claires [❷ / VS]. |
| | **M4.2 – ORGANES**<br>a) Établir le Groupe de coordination cybersécurité [❶ / VS].<br>b) Mettre en place l'Entité cybersécurité VS [❶ / VS]. |
| | **M4.3 – COORDINATION**<br>a) Assurer le suivi de la réalisation des mesures de la CyberStratVS [❶ / VS].<br>b) Assurer la coordination des actions du Valais avec la Confédération et les cantons voisins [❶ / VS].<br>c) Proposer aux parties prenantes, lorsque les opportunités se présentent, la mutualisation de moyens ou le groupement d'achats de biens et de services TIC en matière de cybersécurité [❷ / VS]. |




*Les flèches représentent la durée de la mise en place des actions. Les points symbolisent le moment à partir duquel les actions sont durablement opérationnelles. Les crochets à droite symbolisent la poursuite de ces actions qui s'inscrivent dans la durée.*

Ce planning est tributaire des moyens accordés pour la mise en œuvre de la stratégie et peut donc glisser dans le temps en cas de manque de ressources.

# Annexe 2 - Architecture NIST

Afin de concrétiser les objectifs et intentions de la CyberStratVS, il s'agit de décliner leur réalisation sous forme de mesures. Celles-ci doivent être ordonnées d'une manière rigoureuse et vérifiable selon un canevas connu et appliqué par l'ensemble des acteurs, à savoir celui du NIST qui comprend les six domaines clés suivants :


**Identification** – Chaque entité doit disposer d'une cartographie exhaustive de son cyberespace / de ses structures TIC et de son environnement afin de comprendre ses risques et ainsi de définir ce qui doit être protégé et dans quelle priorité.

**Protection** – Il s'agit de l'ensemble des mesures techniques et non techniques (organisations, processus, etc.) selon les règles de l'art et proportionnées selon les risques identifiés.

**Détection** – Il s'agit ici de rester vigilant, de tester les mesures pour vérifier leur efficacité, d'identifier et annoncer les anomalies, etc., enfin d'agir le plus en amont possible des incidents.

**Réponse** – Une fois une anomalie déterminée / un cyberincident ou une cyberattaque constaté, il s'agit de s'assurer que chaque entité devant être impliquée intervienne le plus rapidement et efficacement possible pour maîtriser la situation, empêcher son extension et minimiser ses conséquences.

**Rétablissement** – L'objectif de cette phase est de revenir le plus rapidement possible à une situation dite « normale » et d'apprendre de la crise afin que les mêmes causes ne puissent plus créer les mêmes effets.

**Gouvernance** – Ce pilier de la cybersécurité est le liant des cinq premiers. Il détermine principalement les buts et effets à atteindre, les ressources dédiées à cet effet et les responsabilités. Il a aussi pour objet de fournir une image d'ensemble de la situation de tous les domaines influant la situation de l'écosystème objet de la stratégie. On dépasse ainsi les seules technologies de l'informations pour considérer tous les domaines pertinents (énergie, personnel, droit, politique, chaînes d'approvisionnement, environnement, etc.).

# Annexe 3 - Abréviations

| | |
|---|---|
| CLDN | Conférence latine des directeurs du numérique |
| CSIRT | Cyber Security Incident Response Team |
| CSN | Cyberstratégie nationale |
| CyberStratVS | Cyberstratégie du canton du Valais |
| GC cysec | Groupe de coordination cybersécurité |
| KPI | Key Performance Indicator (indicateur clé de performance) |
| LIPDA | Loi sur l'information du public, la protection des données et l'archivage |
| LPD | Loi sur la protection des données |
| LPPEx | Loi sur la protection de la population et la gestion des situations particulières et extraordinaires |
| LRens | Loi sur le renseignement |
| LSI | Loi sur la sécurité de l'information |
| LSNA | Loi sur les services numériques des autorités |
| NEDIK | Netzwerk digitale Ermittlungsunterstützung Internetkriminalität |
| NIST | National Institute for Standards and Technology |
| OFCS | Office fédéral de la cybersécurité |
| OCC | Organe cantonal de conduite |
| OCRI | Observatoire cantonal des risques du Canton du Valais |
| SOC | Security Operations Center |