ASSEMBLEA DI CORSICA

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

DELIBERATION N° 26/018 AC DE L'ASSEMBLEE DE CORSE APPROUVANT LA STRATÉGIE CYBERSÉCURITÉ DE LA CORSE

CHÌ APPROVA A STRATEGIA CIBERSICURITÀ DI A CORSICA CYBERCORSICA

SEANCE DU 20 AVRIL 2026

L'an deux mille vingt-six, le vingt avril, l'Assemblée de Corse, convoquée le 8 avril 2026, s'est réunie au nombre prescrit par la loi, dans le lieu habituel de ses séances sous la présidence de Mme Nadine NIVAGGIONI, Vice-présidente de l'Assemblée de Corse.

ETAIENT PRESENTS : Mmes et MM.

Danielle ANTONINI, Véronique ARRIGHI, Serena BATTESTINI, Marie-Claude BRANCA, Paul-Joseph CAITUCOLI, Françoise CAMPANA, Cathy COGNETTI-TURCHINI, Anna Maria COLOMBANI, Romain COLONNA, Christelle COMBETTE, Frédérique DENSARI, Muriel FAGNI, Eveline GALLONI D'ISTRIA, Pierre GHIONGA, Don Joseph LUCCIONI, Antonia LUCIANI, Saveriu LUCIANI, Marie-Thérèse MARIOTTI, Jean-Martin MONDOLONI, Paula MOSCA, Nadine NIVAGGIONI, Antoine-Joseph PERALDI, Marie-Anne PIERI, Jean-Noël PROFIZI, Joseph SAVELLI, Jean-Michel SAVELLI, Charlotte TERRIGHI, Hyacinthe VANNI

ETAIENT ABSENTS ET AVAIENT DONNE POUVOIR :

Mme Marie-Hélène CASANOVA-SERVAS à Mme Muriel FAGNI
Mme Angèle CHIAPPINI à M. Jean-Martin MONDOLONI
Mme Lisa FRANCISCI-PAOLI à Mme Frédérique DENSARI
M. Pierre GUIDONI à Mme Cathy COGNETTI-TURCHINI
Mme Sandra MARCHETTI à Mme Véronique ARRIGHI
Mme Flora MATTEI à Mme Nadine NIVAGGIONI
Mme Marie-Antoinette MAUPERTUIS à M. Hyacinthe VANNI
M. Antoine POLI à M. Saveriu LUCIANI
Mme Juliette PONZEVERA à Mme Antonia LUCIANI
M. Louis POZZO DI BORGO à Mme Anna Maria COLOMBANI
M. Paul QUASTANA à Mme Marie-Claude BRANCA
M. Jean-Louis SEATELLI à M. Jean-Michel SAVELLI
M. François SORBA à M. Antoine-Joseph PERALDI
Mme Elisa TRAMONI à Mme Françoise CAMPANA

ETAIENT ABSENTS : Mmes et MM.

Jean-Christophe ANGELINI, Paul-Félix BENEDETTI, Didier BICCHIERAY, Jean-Marc BORRI, Vanina BORROMEI, Paule CASANOVA-NICOLAI, Santa DUVAL, Petru Antone FILIPPI, Jean-Charles GIABICONI, Josepha GIACOMETTI-PIREDDA, Vanina LE BOMIN, Ghjuvan'Santu LE MAO, Jean-Jacques LUCCHINI, Georges MELA, Jean-Paul PANZANI, Chantal PEDINIELLI, Véronique PIETRI, Pierre POLI, Julia TIBERI, Hervé VALDRIGHI, Charles VOGLIMACCI

L'ASSEMBLEE DE CORSE

VU le Code général des collectivités territoriales, titre II, livre IV, IVème partie, et notamment ses articles L.4421-1 à L.4426-1 et R.4425-1 à D.4425-53,

VU la délibération n° 21/083 AC de l'Assemblée de Corse du 30 avril 2021 portant sur les candidatures au dispositif du plan France Relance Numérique dans le cadre de la politique de transformation et d'aménagement numérique de la Collectivité de Corse,

VU la délibération n° 21/119 AC de l'Assemblée de Corse du 22 juillet 2021 approuvant le cadre général d'organisation et de déroulement des séances publiques de l'Assemblée de Corse, modifiée,

VU la délibération n° 21/195 AC de l'Assemblée de Corse du 18 novembre 2021 adoptant le règlement budgétaire et financier de la Collectivité de Corse,

VU la délibération n° 22/074 AC de l'Assemblée de Corse du 2 juin 2022 approuvant le Schéma Directeur Territorial d'Aménagement Numérique de la Corse - SDTAN Smart Isula,

VU la délibération n° 23/010 AC de l'Assemblée de Corse du 27 janvier 2023 approuvant la stratégie cybersécurité de la Corse et l'adhésion au campus cyber national,

VU la délibération n° 25/206 AC de l'Assemblée de Corse du 18 décembre 2025 portant approbation du budget primitif de la Collectivité de Corse pour l'exercice 2026,

VU la délibération n° 21/154 CP de la Commission Permanente du 28 juillet 2021 approuvant la signature de la convention Plan France Relance en faveur de la création d'un Centre d'urgence cyber territorial (CSIRT) en Corse,

VU la délibération n° 24/168 CP de la Commission permanente du 27 novembre 2024 approuvant la signature de l'avenant de prorogation de la convention France Relance relative à la mise en œuvre du CSIRT CyberCorsica,

VU l'arrêté n°25/650 CE du Conseil exécutif de Corse du 28 octobre 2025 approuvant la signature de la convention relative au financement dans le cadre de l'appel à manifestation d'intérêt « renforcement de l'accompagnement local aux enjeux de cybersécurité » (AMI RALEC) avec le Secrétariat général de la défense et de la sécurité nationale,

SUR rapport du Président du Conseil exécutif de Corse,

VU l'avis n° 2026-05 du Conseil Économique, Social, Environnemental et Culturel de Corse, en date du 17 avril 2026,

VU l'avis n° 2026-05 de l'Assemblea di a Giuventù, en date du 16 avril 2026,

SUR rapport de la Commission du Développement Economique, du Numérique,

de l'Aménagement du Territoire et de l'Environnement,

SUR rapport de la Commission des Finances et de la Fiscalité,

APRES EN AVOIR DELIBERE

A l'unanimité,

Ont voté POUR (42) : Mmes et MM.

Danielle ANTONINI, Véronique ARRIGHI, Serena BATTESTINI, Marie-Claude BRANCA, Paul-Joseph CAITUCOLI, Françoise CAMPANA, Marie-Hélène CASANOVA-SERVAS, Angèle CHIAPPINI, Cathy COGNETTI-TURCHINI, Anna Maria COLOMBANI, Romain COLONNA, Christelle COMBETTE, Frédérique DENSARI, Muriel FAGNI, Lisa FRANCISCI-PAOLI, Eveline GALLONI D'ISTRIA, Pierre GHIONGA, Pierre GUIDONI, Don Joseph LUCCIONI, Antonia LUCIANI, Saveriu LUCIANI, Sandra MARCHETTI, Marie-Thérèse MARIOTTI, Flora MATTEI, Marie-Antoinette MAUPERTUIS, Jean-Martin MONDOLONI, Paula MOSCA, Nadine NIVAGGIONI, Antoine-Joseph PERALDI, Marie-Anne PIERI, Antoine POLI, Juliette PONZEVERA, Louis POZZO DI BORGO, Jean-Noël PROFIZI, Paul QUASTANA, Jean-Michel SAVELLI, Joseph SAVELLI, Jean-Louis SEATELLI, François SORBA, Charlotte TERRIGHI, Elisa TRAMONI, Hyacinthe VANNI

ARTICLE PREMIER :

APPROUVE le rapport du Président du Conseil exécutif de Corse et ses annexes, joints à la présente délibération, relatifs à la définition de la stratégie Cybersécurité de la Corse.

ARTICLE 2 :

APPROUVE l'ajout du livret portant sur la stratégie Cybersécurité de la Corse comme le 12ème Livret du Schéma Directeur Territorial d'Aménagement Numérique de la Corse SMART ISULA figurant en annexe 1 du rapport.

ARTICLE 3 :

AUTORISE le Président du Conseil exécutif de Corse à diffuser et promouvoir la charte CyberCorsica (Annexe 2 du rapport).

ARTICLE 4 :

AUTORISE le Président du Conseil exécutif de Corse à mettre en œuvre la gouvernance CyberCorsica sur la base du règlement intérieur figurant en Annexe 3 du rapport.

ARTICLE 5 :

AUTORISE le Président du Conseil exécutif de Corse à solliciter les crédits contractualisés FEDER et CPER dans le cadre des actions identifiées dans le rapport.

ARTICLE 6 :

La présente délibération fera l'objet d'une publication sous forme électronique sur le site internet de la Collectivité de Corse.

Aiacciu, le 20 avril 2026

La Présidente de l'Assemblée de Corse,

Marie-Antoinette MAUPERTUIS

COLLECTIVITE DE CORSE

RAPPORT
N° 2026/O1/069

ASSEMBLEE DE CORSE

1 ERE SESSION ORDINAIRE DE 2026

REUNION DES 20 ET 21 AVRIL 2026

RAPPORT DE MONSIEUR
LE PRESIDENT DU CONSEIL EXECUTIF DE CORSE

STRATEGIA CIBERSICURITÀ DI A CORSICA CYBERCORSICA

STRATÉGIE CYBERSÉCURITÉ DE LA CORSE CYBERCORSICA

COMMISSION(S) COMPETENTE(S) : Commission du Développement Economique, du Numérique, de l'Aménagement du Territoire et de l'Environnement

Commission des Finances et de la Fiscalité

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

RAPPORT DU PRESIDENT DU CONSEIL EXECUTIF DE CORSE

Préambule

Le présent rapport s'inscrit dans une politique volontariste visant à affirmer la souveraineté numérique de la Corse, un impératif stratégique dans un environnement où le numérique, désormais au cœur des équilibres géopolitiques, est à la fois un levier d'émancipation et un terrain d'influences concurrentes, parfois hégémoniques.

Pour la Corse, la souveraineté numérique repose sur une ambition : protéger les citoyens, les acteurs économiques et les institutions, tout en garantissant un espace numérique de confiance, maîtrisé et propice à l'innovation. Il s'agit de concilier confiance, sécurité des données et liberté d'agir, afin que chacun – particuliers, entreprises ou collectivités – puisse pleinement s'approprier les opportunités offertes par le numérique, sans subir les risques de dépendance ou d'ingérence.

Cette vision s'articule autour de trois piliers déterminants, qui structurent la politique du Conseil exécutif de Corse en matière numérique :

1. La maîtrise des infrastructures numériques. La Corse doit disposer d'infrastructures autonomes, résilientes et au service de l'intérêt général. C'est l'objectif des projets portés par la Collectivité de Corse, notamment la délégation de service public en cours de finalisation (2026), qui vise à déployer et exploiter un socle d'infrastructures souveraines au service du territoire et de ses habitants. Ces infrastructures sont indispensables à une souveraineté effective.

2. La gouvernance des données et de l'intelligence artificielle forme le deuxième pilier de la souveraineté numérique de la Corse. Les données qui constituent une ressource stratégique et l'intelligence artificielle, outil de transformation majeure, doivent être maîtrisées et orientées vers le bien commun. Ce rapport explore précisément ces enjeux, en proposant des pistes pour en faire des leviers au service du développement insulaire, dans le respect des valeurs de transparence et d'éthique portées par la stratégie SMART ISULA.

3. La cybersécurité est un secteur essentiel qui doit garantir une protection vis-à-vis des menaces désormais omniprésentes dans notre espace numérique. Face à la multiplication des cyberattaques, des tentatives de déstabilisation ou des intrusions orchestrées par des acteurs étatiques ou criminels, la Corse se doit de renforcer la protection de ses systèmes, réseaux et données. **Dans ce cadre, la mise en place d'une stratégie de cybersécurité apparaît comme une nécessité pour la Corse.**

En consolidant ces trois dimensions, la Corse affirme sa capacité à construire un numérique souverain – non comme un repli, mais comme une condition de son autonomie et de sa résilience dans un monde de plus en plus interconnecté et numérisé.

Objet du présent rapport

Le Schéma Directeur Territorial d'Aménagement Numérique (SDTAN) de la Corse a été adopté par l'Assemblée de Corse le 2 juin 2022[1]. Intitulé SMART ISULA, il se compose de 11 livrets thématiques[2]. L'ensemble des livrets constitue la stratégie numérique de la Corse d'ici 2032.

SMART ISULA identifiait 4 pistes d'actions rattachées à la Cybersécurité dont l'une s'intitulait : « Élaborer la feuille de route de la politique cybersécurité de la Corse (Action 119) ».

Le présent rapport a pour objet de soumettre à approbation la stratégie Cybersécurité de la Corse - CyberCorsica et de l'inscrire ainsi comme le 12ème Livret du SDTAN de Corse.

Cette stratégie détermine un plan d'action et une trajectoire en matière de Cybersécurité pour les dix prochaines années. Elle a été construite dans le cadre d'une concertation élargie, associant l'ensemble des acteurs publics et privés concernés. Ce dialogue a permis de fédérer les énergies autour des enjeux déterminants de la cybersécurité.

Pour piloter cette réflexion, un comité de suivi a été mis en place en avril 2024 avec pour missions de :

- Dresser un état des lieux de l'écosystème cyber insulaire ;
- Evaluer des scénarios stratégiques adaptés aux besoins du territoire ;

[1] Délibération n°22/074 AC du 2 juin 2022.
[2] Consulter la page https://ambizionedigitale.isula.corsica/le-sdtan-de-corse/

- Esquisser les contours d'un Campus Cyber de la Corse.
- Déterminer une trajectoire opérationnelle à court et moyen terme.

Ce Livret est le fruit de la mobilisation pendant plusieurs mois d'une intelligence collective au service de la stratégie Cybersécurité de la Corse.

La démarche collective engagée

Présentation du livret

Le livret « Stratégie CyberCorsica » est annexé au présent rapport. Il s'organise autour de 4 grands chapitres :

1. La présentation de la démarche,
2. L'état des lieux détaillé de la situation en matière de cybersécurité en Corse,
3. Les enjeux prioritaires de la cybersécurité et les actions associées,
4. Les priorités d'actions pour la période 2026-2028.

Les enjeux prioritaires et actions associées

La stratégie recense 7 enjeux prioritaires :

- Enjeu 1 : Engager une collaboration/coordination entre acteurs de la Cyber en Corse.
- Enjeu 2 : Consolider le tissu professionnel et entrepreneurial Cyber de la Corse
- Enjeu 3 : Offrir un soutien et une protection de proximité à l'ensemble du tissu économique et social insulaire ainsi qu'à sa population.
- Enjeu 4 : Former et accompagner le développement des compétences.
- Enjeu 5 : Acculturer et sensibiliser la société corse aux enjeux Cyber.
- Enjeu 6 : Rendre les infrastructures résilientes et souveraines.
- Enjeu 7 : Créer un Campus Cyber de la Corse.

Elle identifie au total 24 actions, réparties comme suit :

Enjeu	Actions associées
Enjeu 1 : Engager une collaboration/coordination entre acteurs de la Cyber en Corse.	Action 1 : Mettre en place une gouvernance partagée autour d'un collectif CyberCorsica. Action 2 : Déployer une stratégie de marque territoriale CyberCorsica. Action 3 : Diffuser et partager les informations au sein

	du collectif. Action 4 : Mettre en place un observatoire des attaques et des risques Cyber de la Corse. Action 5 : Accompagner l'écosystème au regard des règlementations applicables dans le domaine Cyber. Action 6 : Organiser régulièrement des simulations de crise cyber autour de l'écosystème d'acteurs.
Enjeu 2 : Consolider le tissu professionnel et entrepreneurial Cyber de la Corse	Action 7 : Accompagner les initiatives de structuration collective de la filière Cyber en Corse. Action 8 : Accompagner et valoriser la filière en Corse et hors de Corse. Action 9 : Accompagner les membres de la filière dans leur montée en compétences et leur certification. Action 10 : Accompagner la filière pour attirer les talents et recruter. Action 11 : Créer un lien permanent avec les incubateurs pour détecter et accompagner l'émergence d'entreprises innovantes.
Enjeu 3 : Offrir un soutien et une protection de proximité à l'ensemble du tissu économique et social insulaire, ainsi qu'à sa population.	Action 12 : Mobiliser un accompagnement de proximité et adapté à l'ensemble des organisations et à la population insulaire. Action 13 : Mobiliser/articuler les financements publics en faveur de la Cyber.
Enjeu 4 : Former et accompagner le développement des compétences.	Action 14 : Susciter la création de filières diplômantes dans le domaine du numérique avec un volet cyber affirmé (BAC+2 à BAC+5, écoles d'ingénieurs). Action 15 : Créer une offre de formation tout au long de la vie autour des questions Cyber. Action 16 : Susciter l'émergence de projets de recherche/action autour de la Cyber. Action 17 : Organiser régulièrement des hackathons et défis Cyber pour susciter l'innovation et une formation par la pratique.
Enjeu 5 : Acculturer et sensibiliser la société corse aux enjeux Cyber.	Action 18 : Déployer une animation auprès des jeunes du collège à l'université. Action 19 : Sensibiliser le grand public au cyber, au plus près des territoires. Action 20 : Sensibiliser les organisations publiques et

	privées sur les enjeux Cyber par des actions de proximité. Action 21 : Soutenir la mise en place d'évènements récurrents en lien avec les questions Cyber.
Enjeu 6 – Rendre des infrastructures résilientes et souveraines.	Action 22 : Œuvrer à la résilience et à la souveraineté des infrastructures numériques essentielles de la Corse. Action 23 : Assurer l'alignement de la stratégie cyber avec celle relative à la donnée et à l'intelligence artificielle.
Enjeu 7 – Créer un Campus Cyber de la Corse	Action 24 : Engager la mise en œuvre d'un Campus Cyber de la Corse

Organisation de la gouvernance

Afin de permettre la mise en place d'une gouvernance collaborative, un Comité d'orientation CyberCorsica sera mis en place.

Composé des signataires de la Charte Cybercorsica (ANNEXE 2) et des acteurs engagés dans le développement de la marque territoriale associée, ce Comité aura pour missions de :

- Suivre la mise en œuvre de la Charte et des engagements de CyberCorsica,
- Coordonner et animer la mise en œuvre de l'action collective,
- Accompagner la préfiguration du Campus Cyber de la Corse, en définissant ses axes stratégiques et en consolidant les partenariats nécessaires,
- Garantir une approche inclusive, où chaque acteur peut contribuer à la réflexion et à l'action.

Cette gouvernance participative assure d'une part la cohérence des initiatives, et d'autre part, renforce l'adhésion de tous à une vision commune. Celle-ci est notamment incarnée par les valeurs de la Charte.

En promouvant une gouvernance inclusive et évolutive, le Comité d'Orientation CyberCorsica garantit l'efficacité et la cohérence des actions menées.

Il mobilise l'ensemble des acteurs locaux autour d'une vision commune, renforçant la résilience numérique de la Corse et sa capacité de réponse aux menaces.

Le règlement intérieur de cet organe de gouvernance est annexé au présent rapport (ANNEXE 3)

Plan d’action 2026 2028

Création de la Marque Territoriale CyberCorsica

Dès 2026, la stratégie consiste à élaborer et à développer la marque territoriale CyberCorsica. La marque territoriale CyberCorsica constitue le cadre commun d’identification, de valorisation et de rassemblement des acteurs de la cybersécurité en Corse. Elle ambitionne de valoriser l'excellence corse en matière de cybersécurité tout en fédérant les acteurs insulaires sous une bannière commune.

Son objectif principal est de renforcer l'attractivité de la Corse en la positionnant comme un territoire de référence pour les talents, les entreprises innovantes et les investisseurs. En rassemblant les forces vives de l’île, elle cherche à mobiliser l'ensemble des acteurs afin de créer un écosystème numérique intégré et sécurisé, propice à l'innovation et à la croissance économique.

Pour promouvoir efficacement les compétences insulaires, la marque déploiera des campagnes de communication ciblées, mettant en avant le savoir-faire de la Corse en matière de cybersécurité.

En s’appuyant sur un label de cybersécurité corse, CyberCorsica contribue à renforcer la compétitivité territoriale tout en instaurant un climat de confiance numérique entre les entreprises, les institutions et les citoyens.

Elle consolide ainsi l'image de la Corse comme un territoire numérique de confiance.

Étude pour la mise en place du Campus Cyber de la Corse

La stratégie Cyber pour la Corse comprend un axe majeur consacré à l'étude du Campus Cyber de la Corse dès 2027, projet structurant destiné à fédérer l'écosystème numérique insulaire autour d’un espace d'innovation, de formation et de collaboration.

Inspiré d’autres Campus Cyber, ce projet vise à stimuler l'innovation numérique en réunissant entreprises, startups, institutions académiques et laboratoires de recherche.

En favorisant cette synergie, le Campus ambitionne de développer les compétences en Corse, grâce à des programmes de formation spécialisés en cybersécurité, tout en accélérant l'émergence de startups innovantes dans ce domaine et dans les technologies numériques.

Cette étude stratégique vise également à positionner la Corse comme un pôle d'excellence en cybersécurité, rayonnant au-delà de ses frontières vers le bassin méditerranéen.

Elle portera sur les infrastructures physiques et numériques, les programmes académiques, les espaces de collaboration ainsi que sur les modèles de gouvernance les plus adaptés pour garantir la pérennité et la croissance du Campus.

En consolidant un écosystème numérique intégré et compétitif, cette initiative ambitionne de faire du Campus Cyber de la Corse un catalyseur d'innovation et de compétences en cybersécurité pour le territoire insulaire.

Mobilisation du financement 2026-2028

Les financements ci-dessous correspondent à l'emploi de la subvention versée à la Collectivité de Corse suite à l'arrêté 25/650CE du 28 octobre 2025 portant sur la signature de la convention dans le cadre de l'appel à manifestation d'intérêt « Renforcement de l'accompagnement local aux enjeux de cybersécurité » (AMI RALEC).

Cette subvention d'un montant de 400 000 € prévoit notamment l'affectation des montants suivants :

Accompagnement à la stratégie de marque territoriale :

	DISPONIBLE SUB AMI RALEC	2026	2027	2028
Recrutement sur deux ans d'un chargé de mission affecté à la stratégie Cyber	120 000 €	60 000 €	60 000 €	
Mise en œuvre de la stratégie de communication autour de la marque territoriale CyberCorsica	100 000 €	20 000 €	80 000 €	
TOTAL	220 000 €	80 000 €	140 000 €	

Préfiguration du Campus Cyber :

	Disponible SUB AMI RALEC	2026	2027	2028
Modélisation du campus Cyber de la Corse	10 000 €		10 000 €	

Conclusion

Il est proposé à l'Assemblée de Corse :

- d'approuver le présent rapport et ses annexes ;
- d'approuver l'ajout du livret portant sur la stratégie Cybersécurité de la Corse comme le 12ème Livret du Schéma Directeur Territorial d'Aménagement Numérique de la Corse SMART ISULA figurant en ANNEXE 1 ;
- d'autoriser le Président du Conseil exécutif de Corse à diffuser et promouvoir la charte CyberCorsica (ANNEXE 2) ;
- d'autoriser le Président du Conseil exécutif de Corse à mettre en œuvre la gouvernance CyberCorsica sur la base du règlement intérieur figurant en ANNEXE 3 du présent rapport ;

- d’autoriser le Président du Conseil exécutif de Corse à lancer la marque territoriale CyberCorsica sur la base des financements identifiés dans le présent rapport ;

- d’autoriser le Président du Conseil exécutif de Corse à solliciter les crédits contractualisés FEDER et CPER dans le cadre des actions identifiées dans le présent rapport.

Je vous prie de bien vouloir en délibérer.

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

SMART ISULA

Schéma Directeur Territorial d'Aménagement Numérique de Corse

LIVRET 12

La stratégie cybersécurité de la Corse

Avec le soutien de

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Fonds national d'aménagement et de développement du territoire

Sunta
Sommaire

{ 1 } Préambule

La stratégie cybersécurité de la Corse a été initiée à partir de trois délibérations successives de l'Assemblée de Corse, marquant une démarche progressive et structurée :

- En **2021**, la délibération n°21/083 AC du 30 avril 2021 a acté la candidature de la Collectivité de Corse à l'appel à projets du plan *« France Relance »*, visant la création d'un centre territorial de réponse aux incidents cyber.
- En **2022**, la délibération n°22/074 AC du 2 juin 2022 a arrêté les orientations du *Schéma Directeur Territorial d'Aménagement Numérique (SMART ISULA)*, incluant quatre axes dédiés à la cybersécurité.
- En **2023**, la délibération n°23/010 AC du 27 janvier 2023 a validé l'élaboration d'une stratégie cybersécurité propre à la Corse.

Cette stratégie a été construite dans le cadre d'une **concertation élargie**, associant l'ensemble des acteurs publics et privés concernés. Ce dialogue a permis de **fédérer les énergies** autour d'enjeux déterminants et d'enrichir les orientations initiales de SMART ISULA par **un volet spécifique à la cybersécurité : le présent Livret**.

Pour mener à bien cette réflexion, un **comité de suivi** a été mis en place en **avril 2024**. Il avait pour missions :

- De dresser un **état des lieux** de l'écosystème cyber insulaire ;
- D'évaluer des **scénarios stratégiques** adaptés aux besoins du territoire ;
- D'esquisser les contours d'un **campus Cyber** pour la Corse.
- De déterminer une trajectoire opérationnelle à court et moyen terme.

Ce Livret est donc le fruit de la mobilisation pendant plusieurs mois d'une intelligence collective au service de la stratégie Cybersécurité de la Corse.

{ 2 } Une stratégie cybersécurité pour la Corse

Contexte et objectifs

Le numérique constitue l'un des leviers stratégiques du projet d'autonomie porté par le Conseil exécutif de Corse. Il conditionne la capacité de l'île à s'emparer de son destin pour relever les enjeux d'une société dans laquelle le numérique est devenu incontournable.

Pour cela, l'émancipation de la société insulaire passe nécessairement par un numérique de confiance, protecteur et sûr face aux menaces qui pèsent aujourd'hui sur lui.

Voté en 2022, le Schéma Directeur Territorial d'Aménagement Numérique de la Corse - Smart Isula, identifiait 4 pistes d'actions rattachées à la Cybersécurité :

- Élaborer la feuille de route de la politique cybersécurité de la Corse (Action 119),
- Encourager l'émergence d'un « Campus Cyber » en Corse (Action 70),
- Soutenir les initiatives dans les secteurs Cyber, IA, Datacenter, robotique (Action 88),
- Offrir un soutien opérationnel aux territoires en matière de Cybersécurité (Action 162).

La création du CSIRT (Computer Security Incident Response Team) CyberCorsica[1] et son ouverture opérationnelle en avril 2024 a révélé les besoins de l'ensemble de la société insulaire en matière de protection, de sécurité vis-à-vis des menaces présentes sur les réseaux.

Des initiatives collectives voient le jour en Corse et témoignent d'une mobilisation de l'ensemble des acteurs socio-économiques autour des enjeux de cybersécurité. La création de l'association CLUSIR (Club de la Sécurité de l'Information en Réseau) de Corse affiliée au CLUSIF (Club de la Sécurité de l'Information Français), fin 2023, met en évidence une volonté de fédérer et de travailler ensemble.

1 - Par délibération n°21/154 CP du 22 juillet 2021 le financement de la création d'un CSIRT en Corse a été acté. Basée à Aiacciu, cette unité spécialisée dans la gestion et la réponse aux incidents de cybersécurité est opérationnelle depuis le mois d'avril 2024.

Enfin, les institutions publiques se mobilisent et de nombreux évènements ont été organisés sur l'île autour des questions Cyber comme en témoigne l'état des lieux à venir.

Objectifs de la démarche

Une stratégie Cyber pour la Corse qui défend un numérique protecteur et démocratique pour la Corse et les Corses.

Sans une stratégie Cyber pour la Corse il est illusoire d'envisager la réussite des 192 actions recensées dans le schéma directeur territorial d'aménagement numérique de la Corse SMART ISULA.

Au service de chaque branche de l'Arbre SMART ISULA, de chacune de ses feuilles, la stratégie Cyber de la Corse doit garantir la préservation d'un numérique protecteur et démocratique.

Un numérique protecteur au service de la protection de la vie privée, qui favorise la confiance, lutte et protège contre les fausses informations, les addictions, les vols de données.

Un numérique démocratique au service des libertés fondamentales et de la démocratie, qui assure une maîtrise collective des infrastructures et des systèmes techniques comme des plateformes.

Une stratégie Cyber qui prend en compte les spécificités économiques, sociales, identitaires et culturelles de la Corse comme son caractère d'île-montagne.

Elle doit mettre en perspective cette réalité de terrain, spécifique, dans un contexte mondialisé (géopolitique, règlementaire et technologique) et d'omniprésence du numérique dans les sphères professionnelles ou de vie quotidienne.

Par ailleurs, le tissu entrepreneurial en Corse constitué majoritairement de Très Petites Entreprises (TPE) nécessite de concevoir une offre de service spécifique.

De même, chaque territoire et chaque EPCI doivent être pris en compte dans leur diversité mais aussi au regard des contraintes qui pèsent sur eux.

Enfin, l'émergence d'un tissu de compétences et de prestataires cyber en Corse doit être soutenue en prenant en compte l'étroitesse du marché insulaire et, sans doute, la nécessité de pouvoir répondre à la demande sur l'île et aussi hors de l'île.

Une stratégie Cyber de la Corse qui œuvre à la résilience et la souveraineté numérique de l'île.

Les préoccupations relatives à la souveraineté numérique sont très vives en Europe, en raison de la domination historique des États-Unis, qui s'est traduite par une situation de quasi-monopole technique et économique des multinationales américaines, tant dans le domaine des systèmes d'exploitation que dans celui du développement d'applications.

Pour la Corse la souveraineté numérique correspond à « la maîtrise d'un numérique choisi plutôt que subi ». La Corse et les Corses devant garder la maîtrise de l'orientation de leur usage des technologies et des réseaux informatiques. Cela passe aussi par des infrastructures numériques vues comme des biens communs au service de la Corse. Cette approche de la souveraineté numérique de la Corse est une condition nécessaire à la préservation de ses valeurs. C'est-à-dire une capacité autonome d'appréciation, de décision et d'action dans les usages et services numériques mais aussi la maîtrise des réseaux, des communications électroniques et des données.

Le socle d'infrastructure souveraine constitue un point critique sur lequel il faudra agir de façon à offrir une architecture robuste, résiliente vis-à-vis des menaces. La présence d'un datacenter sécurisé en Corse est passée d'essentielle à vitale.

Une stratégie Cyber de la Corse qui impulse l'émergence d'une offre de services autour d'un campus Cyber

Comme le recommande l'action 70 de Smart Isula intitulée « Encourager l'émergence d'un « Campus Cyber » en Corse », celui-ci devra répondre aux besoins de l'ensemble de l'écosystème insulaire, tout en s'intégrant dans un contexte plus large des Campus Cyber français et européens.

Un Campus Cyber en Corse doit jouer le rôle de catalyseur d'énergie et de compétences au service de l'écosystème Cyber de l'île et être ouvert à des collaborations avec l'ensemble du bassin méditerranéen.

Il pourrait constituer une brique fondatrice - dans le cadre de l'autonomie de la Corse - d'une agence du numérique orientée Données, Intelligence Artificielle et Cybersécurité.

Une stratégie Cyber de la Corse qui stimule les collaborations, les échanges et une gouvernance partagée.

Pour piloter cette démarche, un Comité d'Orientation CyberCorsica sera mis en place. Composé des signataires de la Charte et des acteurs engagés dans la marque territoriale, il aura pour missions de :

- Suivre la mise en œuvre de la Charte et des engagements de CyberCorsica,
- Coordonner et animer la mise en œuvre de l'action collective,
- Accompagner la préfiguration du Campus Cyber, en définissant ses axes stratégiques et en consolidant les partenariats nécessaires,
- Garantir une approche inclusive, où chaque acteur peut contribuer à la réflexion et à l'action.

Cette gouvernance participative assure la cohérence des initiatives et renforce l'adhésion de tous à une vision commune.

En promouvant une gouvernance inclusive et évolutive, le Comité d'Orientation CyberCorsica garantit l'efficacité et la cohérence des actions menées. Il mobilise ainsi l'ensemble des acteurs locaux autour d'une vision commune des enjeux cyber et des moyens à mettre en œuvre pour y répondre.

Cette gouvernance doit également prendre en compte les enjeux et les règlementations françaises et européennes dans le cadre d'une approche complémentaire, subsidiaire et concertée (ex : la directive NIS 2 et sa mise en œuvre en Corse).

{ 3 } Etat des lieux

Ce chapitre dresse un état des lieux qui parcourt cinq éléments :

1. Les forces et faiblesses de la Corse vis-à-vis des enjeux de Cybersécurité ;
2. Les spécificités confrontées à des vulnérabilités et des risques Cyber globalisés ;
3. Un panorama des attaques Cyber ayant touché la Corse ;
4. Un regard sur les entreprises prestataires de services Cyber en Corse ;
5. Un recensement d'initiatives d'acteurs en faveur de la Cyber en Corse.

Forces et faiblesses de la Corse vis à vis des enjeux de Cybersécurité

Une Corse exposée mais qui sait s'adapter

Un premier bilan fait consensus : la Corse présente une **exposition accrue aux risques numériques**, en raison de spécificités socio-économiques marquées.

Des fragilités structurelles avec plusieurs facteurs expliquant cette vulnérabilité :

- Un **tissu économique dominé par les très petites entreprises (TPE)**, moins armées pour faire face aux cybermenaces ;
- Un **maillage communal dense**, avec plus de 360 communes de taille réduite – en moyenne deux fois plus petites que la moyenne française –, souvent dépourvues des ressources nécessaires pour se prémunir efficacement ;
- Une **population plus âgée** par rapport à l'ensemble de la France, plus exposée aux attaques en ligne ;
- Un **niveau de précarité économique élevé**, limitant l'accès à des solutions de protection adaptées ;
- Un **taux de décrochage scolaire supérieur à la moyenne française**, entraînant une moindre sensibilisation des jeunes aux bonnes pratiques numériques.

- Par ailleurs, des **secteurs stratégiques** ont déjà été ciblés par des cyberattaques : éducation, santé, collectivités territoriales, transports, énergie ou encore télécommunications.

Face à ces défis, la Corse démontre une **réactivité remarquable**, portée par une dynamique collective associant acteurs publics et acteurs privés. Cette réactivité se caractérise par :

- Un **écosystème d'acteurs dédié à la cybersécurité** qui arrive à prendre en charge l'essentiel des besoins en la matière ;
- De nombreuses **initiatives associatives** regroupent acteurs publics, entreprises et citoyens autour de cette problématique ;
- Une forte mobilisation autour d'ateliers, **séminaires, conférences et campagnes de sensibilisation**, initiés par des acteurs insulaires et touchant l'ensemble de la société insulaire ;
- Une volonté politique d'implication des **institutions publiques en Corse**, en coordination avec les dispositifs français.

Cette approche concertée permet à la Corse de **surmonter ses handicaps** et de **trouver les solutions adaptées**. Toutefois les problématiques liées à la Cybersécurité ne cessent d'évoluer et de se complexifier. Elles réclament une structuration et un renforcement de l'écosystème Cyber insulaire. C'est tout l'enjeu d'une stratégie Cyber pour la Corse.

Des spécificités confrontées à des vulnérabilités et des risques Cyber globalisés.

Des vulnérabilités globales mises en tension dans un contexte spécifique.

Les vulnérabilités des infrastructures et des systèmes informatiques en Corse reflètent les tendances observées à l'échelle française et internationale, tout en prenant une dimension particulière dans un territoire très marqué par des spécificités géographiques, démographiques, administratives, économiques, identitaires et culturelles.

La Corse, n'échappe pas aux tendances relevées dans rapport annuel sur la cybercriminalité 2025 du ministère de l'Intérieur. Celles-ci étant marquées par une évolution rapide mais aussi une adaptation des attaques.

Un contexte marqué par une cybercriminalité en évolution

Le Rapport d'activité 2024 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) indique que **548 événements liés à la cybersécurité**[1] ont été identifiés entre le 8 mai et le 8 septembre 2024, période couvrant les Jeux olympiques organisés en France. Ces données témoignent de l'ampleur de la menace cyber sur cette période.

Selon ce même rapport, les publics les plus exposés en 2024, tous secteurs confondus, étaient les TPE, les Petites et Moyennes Entreprises (PME), et les Entreprises de Taille Intermédiaire (ETI) ; (37 % des cas), devant les collectivités territoriales (29 %). Ce constat rejoint celui du rapport 2024 de la plateforme cybermalveillance.gouv.fr, *Au coeur de l'action cyber*, qui met en évidence la vulnérabilité particulière des TPE face aux cybermenaces.

Enfin, le Rapport annuel sur la cybercriminalité 2025 du ministère de l'Intérieur indique que la France a enregistré 348 000 cyberattaques en 2024, soit une hausse de 74 % en cinq ans. Ces attaques se concentrent principalement sur :

1 - Les 548 évènements se décomposent en 465 signalements et 83 incidents. Près de la moitié des événements de cybersécurité correspondent à des indisponibilités dont un quart est dû à des attaques par DDoS. Le reste des événements de cybersécurité représente des tentatives de compromission ou des compromissions, des divulgations de données ou bien encore des signalements de vulnérabilités. L'ANSSI précise que les impacts sont restés faibles en raison notamment de la préparation et de la sensibilisation aux risques de cybersécurité réalisées en amont.

- les biens (65 %), incluant les systèmes informatiques et les données ;
- les personnes (29,7 %), via des tentatives de fraude ou d'usurpation d'identité ;
- les institutions et l'ordre public (4,9 %), avec des cibles comme les services publics ou les infrastructures essentielles ;
- les réglementations numériques (0,4 %), telles que les atteintes aux règles de protection des données.

Bien que le nombre de plaintes pour rançongiciels (logiciels bloquant l'accès aux données en échange d'une rançon) ait diminué, leurs méthodes se complexifient. Parallèlement, les vols de données ont affecté plusieurs millions de citoyens, y compris en Corse.

Deux tendances majeures ont été identifiées :

- l'utilisation croissante de l'intelligence artificielle, aussi bien par les cybercriminels que par les acteurs de la défense ;
- la multiplication des actes d'hacktivisme, c'est-à-dire des cyberattaques motivées par des revendications politiques ou géopolitiques.

La France particulièrement touchée en 2025

En France, en 2025, tous les secteurs ont été touchés par des cyberattaques. On dénombre notamment : le Ministère des Sports, le Ministère de l'Intérieur, une vingtaine de fédération françaises du sport, France Travail, plus de 1 000 mairies, une dizaine d'agences régionales de la santé, le Centre National de la Fonction Publique Territoriale, l'Union Nationale du Sport Scolaire, l'Hôpital privé de la Loire, La Sorbonne Université, La Poste, Chronopost, HelloWork, Mondial Relay, Colis Privé , SFR, PornHub, Euromatik, Cuisinella, Médecin Direct, Leroy Merlin, AG2R la Mondiale, Murfy, Michelin, Resana, Pajemploi, Eurofiber, Weda, MYM, Mango, Auchan, Air France, Bouygues Telecom, Louis Vuitton, Disneyland,Cartier, Autosur, Dior, Cerballiance, Carrefour Mobile, Easy Cash, Indigo, Afflelou, Hertz, Harvest, MAIF & BPCE, Intersport…

Source : recensement établi à partir d'un croisement d'informations issues de sources ouvertes, de publications spécialisées et de la veille des acteurs de l'écosystème cyber.

Des fragilités spécifiques à la Corse

L'île présente des vulnérabilités accrues, liées à son **tissu économique et institutionnel** ainsi qu'à son **caractère d'île montagne**.

- **Un sentiment d'être protégé des attaques du fait de l'insularité** : le tissu économique et social a trop souvent le sentiment d'être trop isolé, trop petit pour intéresser les hackers et être la cible d'une attaque. L'insularité donne un faux sentiment de protection vis-à-vis des attaques.
- **Un tissu économique et un secteur public exposés** : les **très petites entreprises** et les **collectivités territoriales**, souvent dotées de moyens limités, peinent à se protéger efficacement.
- Les secteurs de **l'énergie et des transports, déterminants pour l'économie insulaire**, constituent des cibles critiques : leur compromission, même partielle, pourrait avoir des conséquences très préjudiciables à l'ensemble de l'économie de la Corse.
- **Une dépendance critique aux infrastructures de communication** : la Corse ne dispose que de **deux câbles sous-marins** assurant **90 % des échanges numériques** avec le continent. Une interruption de ces liens paralyserait les **services essentiels** (administration, santé, économie) et perturberait gravement la vie quotidienne.
- **Un écosystème cyber encore fragile** : malgré la présence de **prestataires compétents**, leur nombre reste insuffisant pour couvrir les besoins. Les **contraintes budgétaires** des acteurs locaux limitent souvent leur capacité à investir davantage et à recruter.
- **Un manque de visibilité sur les attaques subies** : les **vols de données** touchant des opérateurs publics ou privés (à l'échelle de la France et au-delà) affectent aussi les Corses, sans que ces derniers en soient toujours informés. Faute d'un **recensement exhaustif des attaques**, l'ampleur réelle des cybermenaces sur l'île reste difficile à évaluer. Seules les attaques **médiatisées** ou signalées de manière isolée offrent un aperçu partiel, mais peu significatif.

Panorama des attaques Cyber ayant touché la Corse

La Corse n'est pas épargnée

Afin d'illustrer les vulnérabilités de la Corse en matière de cyber quelques exemples médiatisés dans la presse méritent d'être mentionnés car ils démontrent qu'aucun secteur critique de l'économie insulaire n'a été épargné :

Nom de l'établissement	Secteur économique	Année de l'attaque	Type d'attaque	Source / Statut de l'information
Università di Corsica	Éducation / Recherche	2019	Rançongiciel, demande de rançon	Presse corse + témoignages établissement
SDE2A – Syndicat d'énergie de Corse-du-Sud	Énergie / Collectivité	2019	Cyberattaque par rançongiciel	Rapport d'activité / presse corse
Hôpital de Castelluccio (CH Ajaccio)	Santé publique	2022	Rançongiciel (Vice Society), interruption de services	Presse française & corse, autorités hospitalières
OEHC – Office d'Équipement Hydraulique de la Corse	Gestion de l'eau / établissement public	2022	Cyberattaque par rançongiciel	Communiqué OEHC + presse corse
Corsica Linea	Transport maritime	2022	Attaque informatique (suspicion de rançongiciel)	Citation presse corse
Corsica Ferries	Transport maritime	2023	Rançongiciel + fuite/exfiltration de données (revendication ALPHV/BlackCat)	Presse tech & corse
Collèges de Corse (9 établissements)	Education / établissements publics	2023	Cryptovirus Rançongiciel	Presse corse
Corse GSM	Opérateur de télécommunication	2024	Vol de données	Presse spécialisée

Par ailleurs, la vulnérabilité de la Corse se retrouve aussi dans des vols de données massifs récents, parmi lesquels :

France Travail : en février 2024, l'agence France Travail a subi un important vol de données, avec 43 millions d'informations compromises. Depuis deux autres incidents majeurs, dont le dernier en octobre 2025, ont touché cette agence publique. Dans ce cas les données dérobées sont très sensibles : des identifiants, des mots de passe, des noms, des adresses postales, des adresses mails, des numéros de téléphone, des dates de naissance, des relevés d'identité bancaire, des contrats de travail, des avis d'imposition, des attestations de Sécurité sociale, et des certificats de formation. Des demandeurs d'emploi en Corse ont forcément été les victimes de ce piratage.

Free : début octobre 2024, l'opérateur Free a été victime d'une fuite de données ayant concerné 19 millions d'abonnés (anciens et actuels) incluant des données personnelles (noms, prénoms, adresses, numéros de téléphone...) et plus de 5 millions d'IBAN. Par effet rebond, les milliers d'abonnés Free en Corse ont été victimes de ce piratage.

SFR : fin novembre 2024, les hackers du collectif Near2tlg ont indiqué avoir dérobé les données personnelles de 3,6 millions d'abonnés SFR. Là aussi les données personnelles ont été dérobées (Nom, Prénom, Adresse Email, Adresse postale complète, Date de naissance, Numéro de téléphone). Touchant par effet rebond des milliers de foyers en Corse.

Le CSIRT CyberCorsica : un premier bilan après 20 mois d'activité

Depuis sa mise en place en avril 2024 jusqu'à fin 2025, le CSIRT CyberCorsica a traité 47 incidents significatifs, révélant une menace généralisée et multiforme qui concerne l'ensemble des acteurs socio-économiques de l'île. Ces données soulignent l'importance stratégique de sa mission pour anticiper, détecter et répondre aux cyberattaques.

Les incidents recensés démontrent que :

- Aucune structure n'est épargnée : entreprises, collectivités et associations, quelle que soit leur taille, sont des cibles potentielles.
- Tous les secteurs d'activité sont touchés (tourisme, restauration, transports, enseignement, services à la personne, etc.), sans distinction géographique – des zones rurales aux zones côtières.
- Les méthodes des attaquants évoluent : l'ingénierie sociale (exploitation d'informations publiques sur les sites web ou réseaux sociaux) et les techniques de tromperie (usurpation d'identité, faux contacts hiérarchiques) dominent les stratégies offensives.

Parmi les 47 les incidents suivis par le CSIRT les plus notables se répartissent ainsi :

- 23 % d'escroqueries aux faux virements bancaires (FOVI), aux conséquences financières parfois lourdes pour les victimes.
- 15 % de compromissions de comptes permettant aux attaquants la prise en main du système.
- 13 % d'exploitations de vulnérabilités non corrigées, offrant un accès non autorisé aux systèmes.
- 13 % d'attaques par rançongiciel, bloquant l'accès aux données en échange d'une rançon.
- 10 % de campagnes d'hameçonnage ciblant des données sensibles.
- 10 % d'escroqueries au faux support technique, où les victimes, sous pression, ont laissé un accès prolongé à leurs infrastructures (jusqu'à plusieurs jours).
- 8 % de piratages de sites web ou de pages professionnelles, porte d'entrée vers des attaques plus larges.
- 5 % d'infections par trojan, permettant une prise de contrôle à distance des équipements.
- 5 % de fuites de données, exposant des informations confidentielles.

Ces incidents ont affecté 23 entreprises, 19 collectivités et 4 associations, avec une répartition géographique comme suit : 33 cas en Pumonte et 14 en Cismonte.

Ces chiffres mettent en lumière le rôle essentiel du CSIRT dans :

- L'identification précoce des menaces, grâce à une veille active et à des outils dédiés ;
- L'accompagnement des victimes, pour limiter les dommages et restaurer la confiance ;
- La sensibilisation des acteurs locaux, afin de réduire les dangers liés aux comportements à risque (clics sur des liens frauduleux, partage d'informations sensibles, etc.).

Il faut noter que l'absence d'un décompte précis des attaques en Corse est fortement préjudiciable à la mise en place d'une réponse Cyber appropriée (que ce soit pour les pouvoirs publics comme pour le tissu entrepreneurial local des prestataires Cyber). Un observatoire des attaques en Corse représente un enjeu important que les travaux sur l'état des lieux ont mis en exergue.

Regard sur les entreprises prestataires de services Cyber en Corse

Peu d'entreprises mais une filière investie et combative

L'état des lieux ne visait pas un recensement exhaustif des prestataires de services Cyber basés en Corse. Toutefois, les travaux réalisés estiment leur nombre à une quinzaine d'entreprises tous domaines confondus.

Ces prestataires et ces professionnels de la cybersécurité font face à des défis inédits, liés à la fois aux spécificités insulaires et aux dynamiques plus globales. Bien que les besoins en sécurité numérique et en accompagnement spécialisé ne cessent de croître, les ressources financières d'une grande partie des structures privées comme publiques insulaires restent faibles. Pour surmonter ces obstacles, le réseau des acteurs corses de la cybersécurité doit relever plusieurs défis.

Un marché insuffisamment mâture : le marché insulaire de la cybersécurité reste modeste, principalement en raison de l'insularité et de la faiblesse démographique mais aussi d'une prise de conscience insuffisante des risques numériques, d'un tissu économique de petite taille aux budgets restreints. Cette situation limite le recours aux services spécialisés et ralentit l'émergence d'une offre territoriale diversifiée et pérenne. Pourtant, les prestataires insulaires, bien que confrontés à ces contraintes, restent mobilisés et à la recherche d'opportunités de croissance. Ils s'accordent à reconnaître que leur développement dépendra aussi d'une stratégie corse ambitieuse, portée par les pouvoirs publics, et d'une meilleure sensibilisation des organisations – publiques comme privées – aux enjeux cyber et aux solutions disponibles sur l'île.

Une cohésion des acteurs à trouver : les professionnels corses de la cybersécurité, bien que compétents et interconnectés regrettent un manque de visibilité et de soutien institutionnel. Si des initiatives collectives commencent à se structurer, ils appellent à davantage de synergies et de soutien pour mutualiser leurs ressources, renforcer leur attractivité et saisir des opportunités, tant en Corse qu'à l'extérieur.

Des entreprises cybers très fragiles : le marché insulaire est trop restreint pour permettre aux professionnels de la Cyber en Corse d'atteindre une taille critique. Les jeunes entrepreneurs ont des difficultés à asseoir leur chiffre d'affaires. Ainsi sans une base de clientèle en Corse assurant un chiffre d'affaires minimal, il est difficile de s'implanter durablement.

La pénurie de talents et un déficit de formations : la Corse peine à attirer et à fidéliser des experts en cybersécurité, en raison d'une concurrence accrue et de salaires plus attractifs ailleurs. Pour inverser cette tendance, il est déterminant de déployer des stratégies ciblées : développement de formations en Corse (cursus spécialisés, certifications, reconversions), promotion de l'île comme territoire d'accueil pour les télétravailleurs du secteur, et soutien actif à la filière.

Une dépendance aux prestataires extérieurs : les grands comptes insulaires (collectivités, institutions, entreprises) font souvent appel à des prestataires continentaux, disposant d'une offre plus large. Cette pratique crée une dépendance externe et limite les débouchés pour les acteurs corses. Pour y remédier, il serait judicieux d'encourager les partenariats entre prestataires corses et d'inciter les pouvoirs publics à privilégier, lorsque cela est possible, des solutions insulaires dans leurs appels d'offres.

Un paysage institutionnel complexe : les prestataires évoluent dans un environnement où la multiplicité des interventions publiques nuit à la lisibilité de l'écosystème cyber local et à l'identification de l'offre disponible. La création d'un annuaire officiel des acteurs et des services disponibles en Corse permettrait d'en améliorer la visibilité et d'en faciliter l'accès pour les clients potentiels.

Un soutien public à renforcer : bien que les entreprises bénéficient de dispositifs d'aide publique, peu sont spécifiquement dédiés à la cybersécurité. Des programmes ciblés, comme des démarches de labellisation ou de certification soutenues par l'aide publique seraient essentiels pour structurer et dynamiser cette filière en devenir.

A côté de cela, les prestataires de cybersécurité présents en Corse se distinguent par leur capacité à s'adapter aux besoins insulaires et par leur volonté de se structurer en filière. Quelques points forts de ces acteurs économiques peuvent être mis en lumière :

Une offre complète et diversifiée : l'île dispose d'une gamme étendue de services en cybersécurité, couvrant tous les besoins : protection des données, gestion des incidents, etc. Cette diversité permet de répondre aux spécificités du territoire. Une meilleure coordination entre les acteurs corses renforcerait l'efficacité de ce dispositif.

Des acteurs engagés et innovants : les professionnels corses de la cybersécurité allient engagement territorial et esprit entrepreneurial. Leur attachement à l'île et leur prise de risques contribuent à une offre insulaire résiliente et innovante. Pour amplifier cette dynamique, il sera déterminant de soutenir les démarches de collaboration et de complémentarité entre ces acteurs.

Un engagement fort en faveur de la formation : les acteurs de la filière ont conscience du rôle déterminant de la formation. Ils s'investissent activement dans la formation, en intervenant dans des séminaires, ateliers et sessions dédiées. Ils souhaitent contribuer à créer en Corse un vivier de compétences en cybersécurité, essentiel pour pérenniser la filière.

Des compétences exportables : les entreprises corses possèdent une expertise en cybersécurité susceptible d'être compétitive sur des marchés extérieurs. Valoriser ces savoir-faire à l'international, via des actions de promotion et de mise en réseau, pourrait positionner la Corse comme un pôle de compétences Cyber en Méditerranée.

Une volonté politique affirmée : la Collectivité de Corse veut apporter un soutien actif à la structuration de cette filière. Elle souhaite définir une politique publique efficace et adaptée (subventions, accompagnement à l'innovation) propice au développement d'un écosystème cyber performant.

Des dispositifs globaux qui tendent à s'adapter au territoire : la Corse a accès à des dispositifs français en cybersécurité (notamment ceux de l'ANSSI) qui peu à peu s'adaptent à ses particularités. Ces outils offrent des opportunités en matière de financement, de formation et de mise en réseau. Une meilleure coordination de ces dispositifs avec les dispositifs spécifiques déployés en Corse permettrait d'en optimiser l'impact.

Des initiatives collaboratives en développement : des projets fédérateurs émergent, encourageant la coopération entre les différents acteurs du secteur. Ces démarches collectives favorisent le partage d'expériences et la co-construction de solutions. Pour les consolider, il est important de les organiser en réseaux durables et d'y associer les sphères publiques, privée et académique. Ce mouvement collectif et fédérateur s'amplifie au fil du temps.

Recensement d'initiatives d'acteurs en faveur de la Cyber en Corse

Un écosystème cyber émergent

L'état des lieux réalisé a mis en évidence de nombreuses initiatives structurantes ayant un effet levier sur l'émergence d'un véritable écosystème Cyber en Corse.

Celles recensées ici ne sont pas exhaustives mais veulent seulement témoigner du dynamisme qui anime la communauté des acteurs qu'ils soient publics ou privés.

Le Clusir de Corse : Le CLUSIR Corsica (Club de la Sécurité de l'Information en Réseau Corse) est une association insulaire créée en 2023, affiliée au CLUSIF (Club de la Sécurité de l'Information Français). Son objectif principal est de promouvoir la sécurité de l'information et la cybersécurité en Corse en rassemblant divers acteurs du domaine, tels que des professionnels, des entreprises, des institutions académiques et des organismes publics. Le CLUSIR Corsica organise des événements, des conférences, des ateliers et des formations pour sensibiliser et éduquer ses membres sur les enjeux actuels de la sécurité informatique. Il agit également en tant que relais d'informations et d'alertes sur les menaces numériques affectant le territoire corse.

Le CSIRT CyberCorsica : Le CSIRT CyberCorsica (Computer Security Incident Response Team) est le centre corse de réponse aux incidents de sécurité informatique en Corse. Sa création a été actée par la délibération n°21/154 CP du 22 Juillet 2021. Au sein de la Collectivité de Corse, il mobilise une équipe dédiée de trois personnes. Basé à Aiacciu, le CSIRT CyberCorsica est opérationnel depuis le mois d'avril 2024.

L'action du CSIRT CyberCorsica en quelques chiffres

Depuis son ouverture opérationnelle en avril 2024, après 20 mois de fonctionnement le CSIRT CyberCorsica a :

- Géré 47 incidents de cyber sécurité affectant des Collectivités et entreprises insulaires, quels que soient leur taille, leurs revenus ou leur secteur d'activité.
- Organisé 22 matinées de sensibilisation, réunissant plus de 240 personnes représentant 19 entreprises et 23 collectivités.
- Organisé ou participé à plus de 15 évènements touchant plus de 800 personnes (dont trois jours de conférences et tables rondes « Cyber, IA et Data » dans le cadre des journées Smart Isula en mai 2024).
- Participé à l'exercice massifié de cybersécurité REMPAR25 en septembre 2025 à l'initiative de l'ANSSI.

La Formation certifiante « Les enjeux du numérique et de la cybersécurité » : il s'agit d'un programme de formation intensif de trois jours conçus pour sensibiliser les participants aux défis actuels du numérique et de la sécurité informatique. Elle est organisée par la formation continue de l'Università di Corsica, en partenariat avec l'Agence de Développement Économique de la Corse (ADEC), Airbus et l'association Corsica Sfera. Les sessions de formation ont lieu tous les ans, elles se déroulent à l'IUT di Corsica, à Corti.

La chaire « confiance numérique » de l'Università di Corsica : créée en 2018 au sein de l'Università di Corsica, elle associe des professeurs de droit de cette institution et des avocats associés. Elle aborde la question de la confiance dans les communications électroniques et y associe des sujets liés à la cybersécurité via les services de confiance. Elle organise de nombreux débats en lien avec la cybersécurité, la protection des données personnelles, les services « tiers de confiance ».

Le dispositif « Cyber départ » en Corse : Ce dispositif relève d'une initiative de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) visant à offrir un service gratuit de diagnostic rapide en cybersécurité. Il s'adresse aux entités publiques et privées, quelle que soit leur taille, déjà sensibilisées au risque et souhaitant renforcer concrètement leur cybersécurité. De nombreuses institutions publiques comme la CCI de Corse, le CSIRT sont référents pour conduire les diagnostics sur l'île. Une trentaine d'aidants ont été formés pour conduire les diagnostics (issus du secteur public comme privé). 40 diagnostics ont été réalisés en 2025. D'autres services viendront enrichir cette offre de diagnostic.

L'association CORSICA SFERA : Corsica Sfera est une association dont l'objectif est d'apporter à la Corse de l'information et un réseau d'experts, afin de comprendre et mieux appréhender les enjeux stratégiques, politiques et économiques du monde actuel. Elle se définit comme un think tank et s'intéresse particulièrement aux enjeux liés à l'intelligence économique, la géopolitique, le numérique et la cybersécurité, la gestion de l'information.

Le comité d'action cyber territorial : le comité d'action Cyber (CAC) associe les services de l'Etat et de la Collectivité de Corse. Il vise à harmoniser les actions de sensibilisation aux enjeux de la cybersécurité au sein des entreprises et des

collectivités. C'est également un vecteur d'information au niveau local sur les évolutions règlementaires et les incidents répertoriés sur le territoire insulaire.

Stratégie cyber de la CAPA : A l'initiative de la CAPA des actions sont mises en œuvre à destination des acteurs du territoires afin de les sensibiliser et de les informer. La CAPA a aussi lancé en 2024 le plan « CYBERCAPA » - Plan intercommunal de prévention et de lutte contre la cybercriminalité en faveur des entreprises du territoire.

Le plan « CYBERCAPA - Plan intercommunal de prévention et de lutte contre la cybercriminalité en faveur des entreprises du territoire »

Ce plan est le fruit d'une démarche partenariale associant :

- L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- L'Agence de Développement Économique de la Corse (ADEC) ;
- La Chambre de Commerce et d'Industrie de Corse ;
- La Chambre Régionale de Métiers et de l'Artisanat ;
- La Gendarmerie Nationale ;
- Le CSIRT CyberCorsica ;
- La Direction Générale de la Sécurité Intérieure.

Il s'articule autour de quatre domaines d'action stratégiques :

1. La sensibilisation et l'information des entreprises ;
2. L'accompagnement des entreprises face au risque cyber ;
3. La création et l'animation d'un écosystème cyber local ;
4. La définition d'une gouvernance et d'un pilotage partagé.

Convention ADEC/ANSSI : Signée en 2019, une convention de partenariat autour de la cybersécurité des entreprises entre l'ADEC et l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) initie l'implication Cyber des institutions publiques en Corse,

Journées évènementielles : Elles sont nombreuses, des SECNUMECO, aux Ghjurnate Smart Isula, aux journées ARS Cyber et santé…

Exercice de crise REMPAR25 en Corse : L'exercice REMPAR25 (Renforcement via Exercice Massifié pour Améliorer la Résilience) s'est tenu le 18 septembre 2025 avec une déclinaison en Corse. L'objectif est de sensibiliser les acteurs publics et privés aux enjeux de la continuité d'activité dans un contexte de crise d'origine cyber, de tester les dispositifs existants et s'assurer de la prise en compte du risque cyber. Cinq secteurs étaient ciblés : organisations financières, industries/productions, services publics, administrations publiques/collectivités territoriales, commerces. En Corse une quarantaine de structures ont participé à l'exercice (une dizaine d'organisations dans leur locaux, une vingtaine de participants à la cellule de crise, une dizaine d'institutions partenaires de l'évènement).

Deux BTS avec une composante cyber : Le lycée Laetitia Bonaparte d'Aiacciu ainsi que la cité technique de Montesoru à Bastia offrent chacun une formation technicien supérieur (BTS) dénommée CIEL (Cybersécurité, Informatique et réseaux, Électronique) Option "Électronique et Réseaux" ayant une composante Cybersécurité à leur programme. Toutefois les matières cyber dispensées dans ces deux filières n'ont pu être précisément identifiées dans les descriptifs de leur programme de formation.

Premiers enseignements issus de l'état des lieux

Une Corse encore trop fragile face à l'ampleur des enjeux liés à la Cybersécurité

Les acteurs publics et privés de l'île ont d'ores et déjà engagé des démarches volontaires et collectives pour faire face aux défis de la cybersécurité. Leurs actions couvrent un large spectre : la protection des infrastructures essentielles, la sensibilisation des organisations et des citoyens, l'accompagnement des victimes ou encore l'audit et la sécurisation des systèmes informatiques. Ces initiatives, bien réelles, témoignent d'une volonté d'agir déterminante.

Toutefois cette énergie déployée reste en deçà des enjeux cyber pour la Corse. La montée des attaques et leur complexité, l'omniprésence du numérique dans la vie quotidienne et professionnelle, l'émergence de la Cyberguerre entre les États, la nécessité de protéger tout système numérique qu'elle qu'il soit et l'exposition croissante des populations comme des entreprises rendent la Corse bien fragile face aux défis Cyber.

{ 4 } Les enjeux prioritaires de la cybersécurité

Les enjeux prioritaires présentés ci-après sont le fruit du travail de réflexion mené avec les acteurs insulaires de la cybersécurité réunis dans le comité de suivi CyberCorsica. Ce travail a été nourri de l'état des lieux présenté dans le chapitre précédent.

Ce chapitre présente chacun des enjeux et les pistes d'action qui y sont associées :

Enjeu 1 : Engager une collaboration / coordination entre acteurs de la Cyber en Corse

6 actions

Action 1 : Mettre en place une gouvernance partagée autour d'un collectif CyberCorsica.

Cette action vise à structurer un écosystème collaboratif en Corse en fédérant les acteurs publics, privés, associatifs et académiques autour de la cybersécurité.

L'objectif est de créer une instance de concertation permettant d'harmoniser les initiatives et d'éviter les redondances, tout en définissant des règles de gouvernance claires (Annexe 1).

La charte de la Cyber en Corse étant le socle fédérateur de cette dynamique (son contenu figure en Annexe 2).

Action 2 : Déployer une stratégie de marque territoriale CyberCorsica.

Une marque territoriale CyberCorsica sera mise en œuvre. Elle offrira une identité visuelle et narrative autour de la Cyber en Corse.

Cette marque fédérera les initiatives locales sous une bannière commune autour d'un site vitrine présentant la capacité de la Corse à offrir un numérique souverain et protecteur.

Des campagnes de communication cibleront les investisseurs, les talents et les médias spécialisés, en mettant en avant les initiatives portées en Corse (ex : souveraineté et résilience des infrastructures, service public de la donnée et de l'Intelligence artificielle, projets R&D…). La marque permettra aussi de servir de bannière à des événements (salons, hackathons) et des produits/services CyberCorsica

La marque bénéficiera en priorité aux signataires de la Charte CyberCorsica.

Action 3 : Diffuser et partager les informations au sein du collectif.

Il s'agit de mettre en place un système de partage sécurisé et réactif d'informations entre les membres du collectif (alertes sur vulnérabilités, bonnes pratiques, retours d'expérience).

Une plateforme collaborative dédiée (type intranet ou espace numérique sécurisé) pourra centraliser ces échanges. Des newsletters régulières pourront être élaborées. L'anonymisation des données sensibles et le respect du RGPD seront garantis pour encourager la transparence sans risque juridique.

Dans le même temps, une cellule de veille sera chargée de scanner en continu les opportunités de financement (Europe, État, Collectivités, mécénat) et les marchés publics liés à la Cyber (ex : sécurisation des infrastructures, formation, R&D). Les informations seront diffusées via la plateforme. Un tableau de bord partagé récapitulera les opportunités en cours, leurs montants et les acteurs corses positionnés.

Il sera aussi opportun d'élaborer et de diffuser des kits de sensibilisation CyberCorsica clé en main basés sur les retours d'expérience d'une collectivité et adaptables à d'autres territoires.

Action 4 : Mettre en place un observatoire des attaques et des risques Cyber de la Corse.

Cet observatoire aura pour mission de cartographier en temps réel les cybermenaces pesant sur le territoire (ex : attaques sur les collectivités, ransomware ciblant les hôtels). Il s'appuiera sur des remontées anonymisées des acteurs locaux (via une plateforme sécurisée) et des données ouvertes (ANSSI, CERT). Des rapports semestriels analyseront les tendances (secteurs les plus touchés, typologies d'attaques) et proposeront des recommandations adaptées. Un volet prospectif intégrera des scénarios de risque (ex : impact d'une cyberattaque sur la saison touristique). Les données seront partagées avec les collectifs Cyber pour ajuster les stratégies de prévention.

Cet observatoire pourrait fournir des tableaux de bord partagés permettant le suivi des actions aux différents échelons (territorial, intercommunal, communal).

Une attention particulière devra être portée sur le renforcement des échanges d'information entre les structures Cyber consacrées à la prévention et à l'accompagnement (CSIRT, Prestataires, RSSI…) et les structures ayant pouvoirs de police en matière Cyber (Police et gendarmerie notamment).

Action 5 : Accompagner l'écosystème au regard des règlementations applicables dans le domaine Cyber

Il s'agit d'accompagner l'écosystème en Corse afin qu'il anticipe et se prépare aux réglementations françaises et européennes relatives à la Cyber (ex NIS 2 cf. encart ci-dessous).

La mise en œuvre de ces règlementations est parfois complexe et nécessite une préparation et une information des acteurs pour se conformer à leurs exigences. Ces règlementations sont déterminantes pour aligner la stratégie de la Corse au contexte global, y compris européen, et éviter son déclassement en matière de conformité Cyber.

Une veille règlementaire s'avère essentielle pour mener à bien cette mission.

La directive européenne NIS 2 (2022/2555) (en français : sécurité des réseaux et des systèmes d'Information) vise à renforcer le niveau de cybersécurité des tissus économique et administratif des pays membres de l'UE.

Elle renforce la cybersécurité des réseaux et systèmes d'information, en élargissant son champ aux collectivités territoriales et aux secteurs critiques (eau, énergie, transports, etc.).

Elle impose des obligations strictes en matière de gestion des risques et de déclaration d'incidents.

Pour garantir une proportionnalité de traitement, la directive NIS 2 distingue deux catégories d'entités régulées : les entités essentielles (EE) et les entités importantes (EI), selon leur degré de criticité, leur taille et leur chiffre d'affaires.

Chaque entité régulée devra fournir certaines informations à l'ANSSI, mettre en place des mesures de gestion des risques adaptées, et déclarer ses incidents de sécurité.

Nota : Le décret de transposition de la directive dans le droit français n'est pas publié en février 2026, date d'élaboration du document.

Action 6 : Organiser régulièrement des simulations de crise Cyber autour de l'écosystème d'acteurs en Corse.

Des exercices pratiques seront organisés pour tester la résilience des acteurs face à des scénarios Cyber réalistes (ex : attaque par déni de service sur un port, fuite de données dans une mairie). Ces simulations impliqueront des équipes pluridisciplinaires (techniciens, juristes, communicants) et des coordination croisées (ANSSI, gendarmerie, SDIS…). Un débriefing post-exercice identifiera les points faibles (ex : délais de réaction, coordination) et les axes d'amélioration. Un calendrier annuel sera établi, avec des thèmes variés (ex : crise en période touristique, attaque sur un hôpital). Les retours d'expérience seront capitalisés dans une base de connaissances partagée.

Enjeu 2 : Consolider le tissu professionnel et entrepreneurial Cyber de la Corse.

5 actions

Action 7 : Accompagner les initiatives de structuration collective de la filière Cyber en Corse.

Il s'agit de fédérer les prestataires Cyber (start-ups, TPE/PME, indépendants) autour d'un écosystème cohérent, en créant des synergies entre eux et en jouant sur la complémentarité des compétences (audit, réponse aux incidents, formation, etc.).

L'objectif est de formaliser une dynamique d'association professionnelle ou d'action collective ou de cluster entre ces professionnels. Ceci a pour but de mutualiser les moyens, harmoniser les pratiques et porter une voix unifiée auprès des institutions.

Un diagnostic territorial de la filière pourrait être réalisé.

Il s'agit aussi de soutenir des associations professionnelles (RSSI, DPO, sectorielles…) afin de fédérer les énergies et de parler d'une seule voix.

Action 8 : Accompagner et valoriser la filière en Corse et hors de Corse (en lien avec l'Action 2)

Cette action s'inscrit dans la démarche de marque territoriale CyberCorsica. Elle vise à promouvoir l'expertise insulaire via une stratégie de communication ciblée, mettant en avant des atouts différenciants.

En Corse, des événements comme des salons professionnels ou des webinaires avec des retours d'expérience d'entreprises locales renforceront la visibilité. À l'externe, une participation à des salons nationaux (ex. : FIC, Assises de la Sécurité) ou des partenariats avec des clusters continentaux (ex. : Cyber Campus ou d'autres Cyber Campus implantés dans les régions françaises) ou d'initiatives du type European Digital Information Hub (EDIH) orienté Cyber permettrait l'ouverture de débouchés.

L'objectif est aussi d'élargir le portefeuille clients des entreprises corses en ciblant des secteurs porteurs (ex. : santé, énergie, transport maritime) ou des appels d'offres publics (marchés de l'État, collectivités). Un accompagnement sur mesure serait défini autour d'une **veille stratégique**, d'une **montée en puissance commerciale**, de **réseautage** avec les acteurs Cyber, de projets collaboratifs et d'appels à projets territoriaux ou européens innovants.

Action 9 : Accompagner les membres de la filière dans leur montée en compétences et leur certification

Cette action repose sur un plan de formation adapté aux besoins identifiés (ex. : normes ISO 27001, RGPD, sécurité des systèmes industriels…), avec des modules courts et certifiants pour les professionnels en activité. Des parcours sur mesure, incluant du mentorat par des experts pourraient être organisés.

Parallèlement, un accompagnement à la certification pourrait être proposé et cofinancé par l'aide publique (en priorité les Certifications validées ou proposées par l'ANSSI[1]).

Action 10 : Accompagner la filière pour attirer les talents et recruter

La pénurie de compétences en cybersécurité touche tout le secteur et la Corse en particulier. Il faut donc valoriser les parcours d'immersion pour les étudiants (stages, alternances) en collaboration avec les lycées et les universités et les écoles d'ingénieur en Corse et hors de Corse. Pour attirer des profils expérimentés, des campagnes ciblées et des partenariats avec des plateformes en ligne pourraient être lancés. Un volet "reconversion" pourrait cibler les professionnels du numérique insulaires via des formations accélérées. Enfin, une démarche « observatoire des métiers » permettrait d'ajuster en temps réel les besoins en recrutement et les compétences recherchées.

1 - Label ExpertCyber, Label France Cybersecurity, qualification SecNumCloud, ANSSI PASSI, ANSSI PRIS, ANSSI PACS, ANSII PDIS, labels ISO…..

Action 11 : Créer un lien permanent avec les incubateurs pour détecter et accompagner l'émergence d'entreprises innovantes

Un **lien permanent** sera établi avec les incubateurs insulaires pour identifier et soutenir l'émergence de startups spécialisées en cyber. Des **appels à projets** thématiques (ex : solutions pour les collectivités, outils low-cost pour les TPE) seront lancés, avec un accompagnement renforcé (mentorat, accès à des données tests, mise en relation avec des investisseurs). Un **fond d'amorçage** sera créé pour financer les phases de R&D, et un prix **annuel "Innovation Cyber Corse"** mettra en lumière les projets prometteurs.

Des **résidences d'experts** (hackers éthiques, juristes) pourront être organisées pour stimuler cet écosystème startup.

Enjeu 3 : Offrir un soutien et une protection de proximité à l'ensemble du tissu économique et social insulaire et à sa population

2 actions

Action 12 : Mobiliser un accompagnement de proximité au plus près et adapté à l'ensemble des organisations et de la population insulaire

L'accompagnement de proximité doit être privilégié et identifié par l'ensemble de la société insulaire. Des **relais territoriaux** pourraient aiguiller vers les bons interlocuteurs. L'objectif étant de garantir à chacun une information mais aussi une protection dans le domaine Cyber au plus près et adapté aux spécificités de chacun (des petits commerces, artisans, ou collectivités locales, souvent moins équipés en ressources mais aussi auprès des particuliers et des familles). Une attention particulière étant portée aux **zones rurales et isolées** et aux populations fragilisées.

Des partenariats (Tiers lieux, réseau inclusion numérique, monde associatif ...) pourront jouer un rôle relais mais aussi de sensibilisation.

Enfin, **il faudra que Cybermalveillance se rapproche des territoires** et ait recours à ces dispositifs pour optimiser l'action vis-à-vis des populations.

Action 13 : Mobiliser/articuler les financements publics en faveur de la Cyber.

Cette mesure consiste à élaborer une politique de soutien financier dédiée à la Cyber pour venir en aide au plus grand nombre sur un large panel de sujets.

Cette mesure consiste à **fédérer les dispositifs existants** (État, Collectivités, Europe) pour financer des actions dédiées à la Cyber : diagnostics de vulnérabilité, audits cyber, déploiement de solutions (pare-feu, sauvegardes), réponse aux incidents, obtention de certification et labels.

Elle implique aussi de maintenir les financements sur le long terme et une adaptation des programmes d'aides à l'évolution des risques cyber.

Un **guichet unique** pourrait être créé pour simplifier l'accès aux aides, avec des critères adaptés au tissu des entreprises insulaires. Un **guide des aides** spécifique à la Cyber serait élaboré.

Des **référents territoriaux** seront désignés pour orienter les usagers.

Enjeu 4 : Formation et accompagnement des compétences.

5 actions

Action 14 : Susciter la création de filières diplômantes dans le domaine du numérique avec un volet Cyber affirmé (BAC+2 à BAC+5, écoles d'ingénieur)

Cette action vise à structurer une offre de formation initiale en cyberdéfense, intégrée aux cursus existants ou via des filières dédiées.

L'objectif étant si possible de couvrir tous les niveaux, des BTS/BUT (BAC+2) aux masters (BAC+5) et écoles d'ingénieurs, en partenariat avec l'Università di Corsica et les acteurs nationaux (ANSSI, écoles spécialisées). Ces filières devront inclure des modules pratiques (simulations d'attaques, gestion de crise) et des stages en entreprise pour répondre aux besoins des secteurs publics et privés insulaires.

Une attention particulière sera portée à l'attractivité de ces formations pour les étudiants locaux et continentaux, via des bourses ou des conventions avec les employeurs corses.

Action 15 : Créer une offre de formation tout au long de la vie autour des questions Cyber (En lien avec l'Action 9).

Cette action cible les professionnels en poste (agents territoriaux, salariés d'entreprises, indépendants) pour les sensibiliser et les monter en compétence sur les enjeux cyber (RGPD, protection des données, sécurisation des systèmes). Les formations, modulaires et certifiantes, seront coconstruites avec les branches professionnelles (tourisme, santé, agriculture) et les collectivités, en s'appuyant sur des organismes agréés. Des sessions en présentiel et en distanciel seront proposées, avec un volet spécifique pour les élus et cadres dirigeants. Un dispositif de financement pourra être mis en place pour lever les freins à l'accès.

Pour positionner la Corse comme un territoire d'expertise cyber en Méditerranée, des formations haut de gamme (Master Class) pourront être organisées, animées par des intervenants nationaux et internationaux (experts ANSSI, chercheurs, hackers éthiques). Ces cycles cibleront des thématiques précises (cybersécurité industrielle, lutte contre la cybercriminalité, souveraineté numérique) et s'adresseront aux professionnels confirmés.

Action 16 : Susciter l'émergence de projets de recherche/action autour de la Cyber (en lien avec l'Action 11).

Il s'agit par cette action d'encourager les synergies entre laboratoires de recherche et acteurs socio-économiques pour développer des projets appliqués en cybersécurité. Les axes prioritaires incluront la protection des infrastructures critiques (ports, énergie, télécommunication), la sécurisation des données touristiques, ou l'adaptation des outils cyber aux spécificités insulaires (réseaux isolés, saisonnalité). Les résultats seront valorisés via des publications et des transferts vers les entreprises locales.

Action 17 : Organiser régulièrement des hackathons et défis Cyber pour susciter l'innovation et une formation par la pratique

Ces événements, ouverts aux étudiants, startups et professionnels, auront pour but de résoudre des problèmes concrets (ex : sécurisation d'une plateforme de réservation touristique, détection de vulnérabilités dans un réseau communal). Organisés en partenariat, ils combineront compétition, mentorat et networking. Les lauréats bénéficieront d'un accompagnement pour industrialiser leurs solutions (aides à l'innovation, accès à des fonds territoriaux). Une édition annuelle "CyberCorsica Challenge" sera médiatisée pour sensibiliser le grand public et attirer des talents extérieurs.

Enjeu 5 : Acculturer et sensibiliser la société Corse aux enjeux Cyber

4 actions

Action 18 : Déployer une animation auprès des jeunes du collège à l'université.

Cette action vise à intégrer les enjeux de cybersécurité dans les parcours éducatifs des jeunes Corses, du collège à l'enseignement supérieur. Des ateliers interactifs (jeux de rôle, défis en ligne, simulations de cyberattaques) seront organisés en partenariat avec les établissements scolaires et les acteurs locaux du numérique et de la Cyber. L'objectif étant de développer une culture du risque cyber (protection des données, identification des fake news, bonnes pratiques sur les réseaux sociaux) tout en suscitant des vocations dans les métiers de la cybersécurité. Une attention particulière sera portée aux filières technologiques (BTS IUT, écoles d'ingénieurs) pour renforcer les compétences locales. Des kits pédagogiques clairs et adaptés à chaque niveau seront mis à disposition des enseignants.

Action 19 : Sensibiliser le grand public à la Cyber au plus près des territoires

Cette initiative s'appuie sur les **tiers lieux** (fab labs, espaces publics numériques,

médiathèques) et les acteurs de la médiation (associations, CCAS) pour toucher un public large, y compris les seniors et les publics éloignés du numérique. Des sessions thématiques (ex : « FakeNews », "Sécuriser ses comptes en ligne", "Reconnaître un phishing") seront proposées sous forme d'ateliers pratiques ou de cafés-débats, avec des supports multilingues (français, corse). Une campagne de communication ciblée (affiches, réseaux sociaux, partenariats avec les mairies) accompagnera le déploiement. L'accent sera mis sur les **usages du quotidien** (e-administration, e-commerce) pour ancrer les réflexes de vigilance.

Action 20 : Sensibiliser les organisations publiques et privées sur les enjeux Cyber par des actions de proximité

Destinée aux **collectivités**, **entreprises (TPE/PME) et administrations**, cette action propose des **diagnostics allégés** des vulnérabilités suivis de recommandations pratiques. Des rencontres sectorisées (ex : tourisme, santé, agriculture) permettront d'aborder des cas concrets (ex : protection des données clients, sécurisation des paiements en ligne). Cette **action est aujourd'hui investie fortement par le CSIRT CyberCorsica** notamment qui pourrait jouer ici le rôle d'assembleur d'initiatives en Corse.

Action 21 : Soutenir la mise en place d'évènements récurrents en lien avec les questions Cyber (En lien avec l'Action 2)

Pour ancrer la cybersécurité dans le paysage insulaire, cette action prévoira l'organisation d'**évènements annualisés** :

- Un **forum "CyberCorsica"** réunissant experts, institutions et grand public autour de conférences et démonstrations (ex : hackathon éthique, village des métiers).
- Des **séminaires thématiques** pour les élus et cadres (ex : "Cyber et transition numérique des territoires", "RGPD et collectivités").
- Des évènements dans le cadre d'un **mois de la cybersécurité** en octobre, en écho au **European Cybersecurity Month**.

Ces évènements étant coconstruits avec les acteurs de l'écosystème Cyber en Corse et dans le cadre de l'action de marque territoriale CyberCorsica.

Enjeu 6 – Des infrastructures résilientes et souveraines.

Action 22 : œuvrer à la résilience et à la souveraineté des infrastructures numériques essentielles de la Corse

L'objectif consiste à assurer une maîtrise des infrastructures de télécommunications et de transport et d'hébergement essentielles à la Corse.

La Corse doit disposer d'infrastructures sécurisées, autonomes, résilientes et au service de l'intérêt général. C'est l'objectif des projets portés par la Collectivité de Corse en matière de très haut débit, de liens Corse continent…. La délégation de service public en cours visant à déployer et exploiter un socle d'infrastructures souveraines au service du territoire et de ses habitants devrait être attribuée courant 2026. Elle constitue un des leviers indispensables à une souveraineté effective de la Corse en matière d'infrastructures et aussi d'hébergement de données.

La Collectivité de Corse doit s'attacher à l'élaboration d'un plan de résilience et de sécurisation de ses infrastructures.

Action 23 : Assurer l'alignement de la stratégie Cyber avec celle relative à la donnée et à l'intelligence artificielle

L'objectif consiste à assurer la prise en compte des questions cyber dans la gestion du service public de la donnée et de l'intelligence artificielle de la Corse.

Il s'agit d'assurer la synergie des composantes Cyber, Data et Intelligence Artificielle qui demeurent indissociables dans le cadre d'une souveraineté numérique de la Corse.

Ainsi la charte CyberCorsica doit être en résonnance avec la charte de la donnée et de l'IA.

De même le service public de la donnée et de l'Intelligence artificielle de la Corse ne pourra se déployer sans faire appel à un environnement sécurisé.

Dans ce cadre des passerelles doivent se créer entre les différents acteurs et aussi les organes de gouvernance. La préfiguration d'une structure de type agence du numérique regroupant les problématiques IA, Data et Cyber pourrait représenter un scénario possible à intégrer dans la réflexion autour du campus Cyber (enjeu 7).

Enjeu 7 – Un campus Cyber pour la Corse

Action 24 : engager la mise en œuvre d'un Campus Cyber pour la Corse

La création d'un Campus Cyber en Corse est un objectif à atteindre. Il est nécessaire à terme de créer une structure pivot susceptible de porter les actions mais aussi de fédérer et de faire évoluer l'écosystème Cyber en Corse.

Ce Campus aura pour vocation de fédérer au sein d'un espace dédié à l'innovation, à la formation et à la collaboration. Inspiré des initiatives menées par ailleurs, il réunira entreprises, startups, établissements d'enseignement supérieur et laboratoires de recherche pour stimuler l'innovation numérique et renforcer l'écosystème insulaire en cybersécurité. Grâce à des programmes de formation spécialisés et à un accompagnement des jeunes pousses, il contribuera à conforter la capacité de la Corse à répondre aux défis à venir.

Au-delà de son ancrage territorial, le Campus Cyber de la Corse vise à positionner l'île comme un pôle reconnu en cybersécurité, en synergie avec les acteurs du bassin méditerranéen.

Il sera le hub autour duquel un écosystème Cyber intégré et pérenne pourra disposer :

- des infrastructures physiques et numériques adaptées,
- de programmes de formations académiques et professionnelles,
- d'espaces de coworking et de collaboration,
- d'une gouvernance équilibrée,
- d'un modèle économique assurant sa viabilité à long terme.

Le Campus sera aussi le levier de la mise en œuvre coordonnées de l'ensemble des actions présentées dans le présent livret.

Synthèse des enjeux et des actions

La stratégie Cyber de la Corse repose ainsi sur 24 actions structurées autour de 7 grands enjeux.

- Enjeu 1 : Engager une collaboration/coordination entre acteurs de la Cyber en Corse.
- Enjeu 2 : Consolider le tissu professionnel et entrepreneurial Cyber de la Corse
- Enjeu 3 : Offrir un soutien et une protection de proximité à l'ensemble du tissu économique et social insulaire et à sa population.
- Enjeu 4 : Formation et accompagnement des compétences.
- Enjeu 5 : Acculturer et sensibiliser la société Corse aux enjeux Cyber.
- Enjeu 6 : Des infrastructures résilientes et souveraines.
- Enjeu 7 : Un campus Cyber pour la Corse.

Enjeu	Action associée
Enjeu 1 : Engager une collaboration/ coordination entre acteurs de la Cyber en Corse.	Action 1 : Mettre en place une gouvernance partagée autour d'un collectif CyberCorsica. Action 2 : Déployer une stratégie de marque territoriale CyberCorsica. Action 3 : Diffuser et partager les informations au sein du collectif. Action 4 : Mettre en place un observatoire des attaques et des risques Cyber de la Corse. Action 5 : Accompagner l'écosystème au regard des règlementations applicables dans le domaine Cyber. Action 6 : Organiser régulièrement des simulations de crise Cyber autour de l'écosystème d'acteurs.
Enjeu 2 : Consolider le tissu professionnel et entrepreneurial Cyber de la Corse	Action 7 : Accompagner les initiatives de structuration collective de la filière Cyber en Corse. Action 8 : Accompagner et valoriser la filière en Corse et hors de Corse Action 9 : Accompagner les membres de la filière dans leur montée en compétences et leur certification. Action 10 : Accompagner la filière pour attirer les talents et recruter. Action 11 : Créer un lien permanent avec les incubateurs pour détecter et accompagner l'émergence d'entreprises innovantes
Enjeu 3 : Offrir un soutien et une protection de proximité à l'ensemble du tissu économique et social insulaire et à sa population.	Action 12 : Mobiliser un accompagnement de proximité au plus près et adapté à l'ensemble des organisations et de la population insulaire. Action 13 : Mobiliser/articuler les financements publics en faveur de la Cyber.

Enjeu	Action associée
Enjeu 4 : Formation et accompagnement des compétences.	Action 14 : Susciter la création de filières diplômantes dans le domaine du numérique avec un volet Cyber affirmé (BAC+2 à BAC+5, écoles d'ingénieur). Action 15 : Créer une offre de formation tout au long de la vie autour des questions Cyber Action 16 : Susciter l'émergence de projets de recherche/ action autour de la Cyber Action 17 : Organiser régulièrement des hackathons et défis Cyber pour susciter l'innovation et une formation par la pratique
Enjeu 5 : Acculturer et sensibiliser la société Corse aux enjeux Cyber.	Action 18 : Déployer une animation auprès des jeunes du collège à l'université. Action 19 : Sensibiliser le grand public à la Cyber au plus près des territoires. Action 20 : Sensibiliser les organisations publiques et privées sur les enjeux Cyber par des actions de proximité Action 21 : Soutenir la mise en place d'évènements récurrents en lien avec les questions Cyber.
Enjeu 6 – Des infrastructures résilientes et souveraines.	Action 22 : œuvrer à la résilience et à la souveraineté des infrastructures numériques essentielles de la Corse. Action 23 : Assurer l'alignement de la stratégie Cyber avec celle relative à la donnée et à l'intelligence artificielle.
Enjeu 7 – un campus Cyber pour la Corse	Action 24 : engager la mise en œuvre d'un Campus Cyber pour la Corse.

{ 5 } Priorités d'actions pour la période 2026-2028

Dans un premier temps quatre leviers seront actionnés afin d'activer les différentes actions identifiées :

- La diffusion d'une charte Cybersécurité pour la Corse,
- La mise en œuvre d'une démarche de marque territoriale CyberCorsica,
- L'organisation de la gouvernance,
- La préfiguration d'un Campus Cyber en devenir.

C'est sur cette base qu'ont été identifiées les actions et enjeux prioritaires de la période 2026-2028.

Les pistes d'actions prioritaires

Les **actions 1, 2, 3, 4, 5, 6** afférentes à l'enjeu 1 constituent les bases fondatrices de la dynamique 2026-2028. La Collectivité de Corse s'investira comme coordinatrice et animatrice de ces actions afin de poser les fondations d'un collectif agissant.

L'action 7 de l'enjeu 2, est prioritaire et conditionne la réalisation des actions 8, 9, 10, 11. Elle correspond à la volonté des prestataires de service Cyber en Corse de s'organiser opérationnellement en filière. Des règlements d'aides sont déjà disponibles pour l'organisation en filière. Il faudra œuvrer à les recenser et à en faciliter l'accès afin que celle-ci émerge au plus tôt.

Concernant **l'action 12**, le CSIRT CyberCorsica travaille déjà à fédérer les acteurs afin d'organiser plus efficacement le soutien, l'accompagnement et la réponse à incident.

L'action 13 de l'enjeu 3, est prioritaire, elle nécessite la mise en place d'une ingénierie de l'aide publique afin de fournir une offre de soutien multi-service adaptée à chacun. Les crédits contractualisés FEDER et CPER devront être mobilisés.

L'enjeu 5 doit tout d'abord se structurer autour de la construction d'une offre de service de médiation Cyber disponible sur tous les territoires et touchant l'ensemble de la société insulaire. Pour cela il faudra mobiliser le système éducatif insulaire, le réseau des tiers lieux, celui de la médiation numérique. Il faudra aussi développer des partenariats avec des partenaires comme le CNNUM ou l'association LUMINIQUE afin de disposer de kits de médiation et de cursus de formation d'animateurs Cyber.

L'enjeu 6, nécessite d'entamer l'élaboration d'un plan de résilience et de sécurisation des infrastructures numériques essentielles de la Corse.

L'enjeu 7 reste une cible à atteindre. Le déploiement de ces actions permettra d'alimenter la définition fine du périmètre de l'offre de service du Campus Cyber de la Corse ainsi que son modèle économique et le véhicule juridique associé.

Financements publics mobilisables pour la période 2026-2028

L'aide publique en faveur de la stratégie Cyber de la Corse pour la période 2026-2028 pourra mobiliser les dispositifs suivants :

Programmes opérationnels FEDER 2021-2027

Deux mesures sont consacrées au numérique :

Volet numérique du FEDER 2021-2027	Enveloppe contractualisée FEDER 201-2027
Objectif Spécifique RSO1.2 : Tirer parti des avantages de la numérisation au bénéfice des citoyens, des entreprises, des organismes de recherche et des pouvoirs publics	6 710 000 €
Objectif Spécifique RSO1.5 : Renforcer la connectivité numérique	5 000 000 €
Total	11 710 000 €

Une mobilisation de l'OS Spécifique RSO 1.2 à hauteur de **2 000 000 €** de crédits FEDER autour des axes suivants était envisagée :

- Soutien au fonctionnement du CSIRT,
- Mise en œuvre du Campus Cyber,
- Soutien aux diagnostics et audits d'organisation

Contrat de plan Etat Collectivité de Corse 2021-2027

Le contrat de plan Etat-Collectivité de Corse 2021-2027 dispose d'un volet numérique financé à hauteur de 3 000 000 € selon la répartition ci-après :

Volet numérique	Enveloppe contractualisée CPER 201-2027
Participation financière de l'État	1 500 000 €
Participation financière de la Collectivité de Corse	1 500 000 €
Total	3 000 000 €

Le volet numérique du contrat de plan intègre une mesure consacrée à la Cyber. Elle s'intitule « Développement d'un pôle territorial sur la cybersécurité » et cible les actions suivantes :

- Assurer la pérennité du CSIRT et son rayonnement territorial ;
- Accompagner le développement d'une structure d'intérêt général sur le modèle d'un Cyber Campus susceptible de :
- Contribuer au développement des « communs » de la cybersécurité ;

- Soutenir la recherche et l'innovation ;
- Développer la formation en cybersécurité et susciter des vocations ;
- Renforcer la coopération en matière opérationnelle.

Une mobilisation du contrat de plan l'ordre de **1 000 000 €** (0,5K€ Etat, 0,5K€ CdC) est envisageable.

AMI RALEC ANSSI

L'ANSSI a lancé le 22 août 2025 un appel à manifestation d'intérêt, intitulé « Renforcement de l'accompagnement local aux enjeux de cybersécurité » (AMI RALEC). La candidature de la Collectivité de Corse, déposée le 19 septembre 2025, a été sélectionnée le 6 octobre 2025. Dans ce cadre une subvention de **400 000 €** a été versée pour financer entre 2026 et 2027 les actions suivantes :

Actions financées dans le cadre de l'AMI RALEC	Montant financier
Renforcement de l'action du CSIRT CyberCorsica	170 000 €
Recrutement d'un chargé de mission affecté à la stratégie Cyber	120 000 €
Mise en œuvre de la stratégie de communication autour de la marque territoriale CyberCorsica	100 000 €
Modélisation du campus Cyber de la Corse	10 000 €
Total	400 000 €

Décomposition des sources de financement mobilisables

Sources	Enveloppe totale	Enveloppe mobilisable
Volet Numérique du FEDER 2021 2027 Objectif Spécifique RSO1.2	6 710 000 € de crédits FEDER	2 000 000 €
Contrat de plan Etat-Collectivité de Corse 2021 2027 - volet numérique	3 000 000 € de crédits Etat Collectivité de Corse	1 000 000 €
AMI RALEC ANSSI	400 000 €	400 000 €
Total		400 000 €

Autres sources de financement et initiatives locales

Les autres sources de financement mobilisable adressent en particulier des budgets spécifiques que chaque acteur public souhaite allouer à l'accompagnement de la stratégie Cyber de la Corse.

Il s'agit de crédits inscrits au budget de l'institution publique qui peuvent soit bénéficier d'un cofinancement dans le cadre des mesures présentées plus haut ou ne bénéficier d'aucun cofinancement.

Mobilisation des financements

Les financements de la stratégie Cyber doivent assurer une articulation des financements contractualisés ou territoriaux avec les initiatives locales. Pour cela il sera nécessaire :

- De clarifier les modalités d'accès à ces financements pour les collectivités locales engagées dans des démarches cyber ;

- De jouer la complémentarité des financements et des sources de financement.
- D'identifier des enveloppes dédiées au soutien des initiatives territoriales existantes
- De concerter avec l'ensemble des acteurs publics la répartition des financements et le montage de dossiers de financement
- D'étudier la possibilité de création d'un fonds dédié Cyber destiné aux TPE en particulier facilitant une prise de conscience (pré diagnostic) et un rattrapage de leur maturité de leur système informatique en sécurité (post diagnostic).

{ 7 } Conclusion

Dans un contexte mondialisé marqué par l'accélération de la transformation numérique et la multiplication des cybermenaces, la Corse devait se doter d'une stratégie Cyber. Cette stratégie ayant comme objectifs de renforcer la protection de ses infrastructures essentielles, bâtir un écosystème numérique fiable et sûr afin de préserver et protéger la Corse et les Corses, leur données, leurs valeurs éthiques, sociales et culturelles.

Elle s'inscrit pleinement dans la vision Smart Isula, où le numérique devient un levier d'émancipation, au service de l'autonomie et de l'attractivité de l'île. En unissant ses forces, la Corse aspire à devenir un modèle de résilience et de souveraineté numérique dans le respect de ses valeurs.

Élaborée de manière collaborative, cette stratégie a voulu rassembler les points de vue d'acteurs publics, privés, académiques et associatifs autour d'objectifs communs en matière de cybersécurité.

Cette stratégie ne peut se réaliser sans la complémentarité avec les dynamiques des territoires avec la mise en place de mécanismes de coordination permettant une véritable co-construction.

C'est sur ce principe que devront se mettre en œuvre les 7 enjeux et les 24 actions identifiées. En ce sens quatre leviers seront actionnés au plus tôt :

- La diffusion de la charte Cybersécurité pour la Corse pour fédérer la communauté ;
- La mise en œuvre d'une démarche de marque territoriale CyberCorsica ;
- L'organisation de la gouvernance ;
- La préfiguration d'un Campus Cyber en devenir.

1 - La Charte Cybersécurité : un engagement collectif autour d'une vision partagée

La Charte Cyber de la Corse constitue le socle de valeurs sur lequel se fonde l'adhésion à un collectif et la mise en œuvre d'actions qui en découlent.

La charte, ne s'impose pas ; elle est basée sur l'engagement volontaire de chacun. Elle vise à fédérer l'ensemble des acteurs insulaires autour de principes collectivement acceptés en matière de cybersécurité.

Elle favorise la création d'une dynamique collective et encourage la coopération entre acteurs publics, privés, associatifs et académiques. Elle favorise également l'adoption de bonnes pratiques en cybersécurité en respectant les spécificités de la Corse.

En mobilisant les acteurs du territoire, cette charte contribue à renforcer la résilience et la souveraineté numérique de la Corse en même temps qu'elle stimule une intelligence collective.

2 - CyberCorsica : une marque territoriale pour valoriser une intelligence collective autour de la Cyber

La marque territoriale CyberCorsica sera guidée par sa Charte Cyber. Elle ambitionne de rassembler les acteurs corses de la cybersécurité sous une identité commune pour mettre en lumière l'excellence du territoire dans ce domaine.

Cette initiative vise à stimuler et structurer les compétences, l'innovation et l'entrepreneuriat en matière Cyber. Elle veut ainsi attirer les talents et instaurer un climat de confiance dans l'univers digital, au bénéfice des entreprises, des institutions et des citoyens.

En fédérant les forces vives du territoire, CyberCorsica offre une visibilité et une cohérence aux actions menées en cybersécurité. Elle permet aussi de créer un écosystème solidaire, où les acteurs les plus expérimentés soutiennent les plus faibles permettant ainsi d'atteindre une masse critique qui manque souvent à la Corse.

Pour valoriser ce savoir-faire insulaire, la marque déploiera des campagnes de communication ciblées, mettant en avant les atouts locaux. Elle favorisera le dialogue et le partage de valeurs communes entre tous les acteurs, consolidant ainsi l'image de la Corse comme un territoire numérique fiable et innovant.

3 - Un Campus Cyber en Corse pour fédérer, former et innover

La création d'un Campus Cyber en Corse s'appuiera sur le déploiement de la marque territoriale « CyberCorsica », dont l'adoption sera un levier déterminant pour sa réussite. En parallèle, les contours de ce projet structurant seront définis avec précision : offre de services, modèle économique et cadre juridique associés.

Ce Campus aura pour vocation de fédérer les acteurs du numérique insulaire au sein d'un espace dédié à l'innovation, à la formation et à la collaboration lié à la question Cyber. Inspiré des initiatives menées par ailleurs, il réunira entreprises, startups, établissements d'enseignement supérieur et laboratoires de recherche pour stimuler l'innovation numérique et renforcer les compétences corses en cybersécurité. Grâce à des programmes de formation spécialisés et à un accompagnement des jeunes pousses, il contribuera à l'émergence d'un tissu économique dynamique dans ce domaine et les technologies associées.

Au-delà de son ancrage territorial, le Campus Cyber de la Corse vise à positionner l'île comme un pôle reconnu en cybersécurité, en synergie avec les acteurs du bassin méditerranéen.

4 - Une gouvernance collaborative pour « faire ensemble »

Pour piloter cette démarche, un Comité d'Orientation CyberCorsica sera mis en place. Composé des signataires de la Charte et des acteurs engagés dans la marque territoriale, il aura pour missions de :

- Suivre la mise en œuvre de la Charte et des engagements de CyberCorsica,
- Coordonner et animer la mise en œuvre de l'action collective,
- Accompagner la préfiguration du Campus Cyber, en définissant ses axes stratégiques et en consolidant les partenariats nécessaires,
- Garantir une approche inclusive, où chaque acteur peut contribuer à la réflexion et à l'action.

Cette gouvernance participative assure la cohérence des initiatives et renforce l'adhésion de tous à une vision commune incarnée notamment par les valeurs de la Charte.

En promouvant une gouvernance inclusive et évolutive, le Comité d'Orientation CyberCorsica garantit l'efficacité et la cohérence des actions menées. Il mobilise ainsi l'ensemble des acteurs locaux autour d'une vision commune, renforçant la résilience numérique de la Corse et sa capacité de réponse aux menaces.

Vos projets

Vos contributions

Vos projets

Vos contributions

Mentions légales

Schéma Directeur Territorial d'Aménagement Numérique de la Corse - Smart Isula
Version 1.0 de novembre 2025

Date de publication : novembre 2025

Éditeur : Cullettività di Corsica - Collectivité de Corse - 22, cours Grandval BP 215 - 20187 Aiacciu cedex ▪ Directeur de publication : le Président du Conseil exécutif de Corse ▪ Responsable d'édition : la Direction de la Transformation Numérique de la Corse ▪ Conception graphique : Benjamin Gour (Corsica Lab) ▪ Rédaction : l'équipe de la Direction de la Transformation Numérique avec le concours de l'entreprise SYNEOR.

Ce document est disponible en téléchargement sur le site
https://ambizionedigitale.isula

SMART ISULA

Schéma Directeur Territorial
d'Aménagement Numérique de Corse

LIVRET 12

La stratégie cybersécurité de la Corse

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

www.smart-isula.corsica

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

SMART ISULA

Schéma Directeur Territorial d'Aménagement Numérique de Corse

Charte CyberCorsica

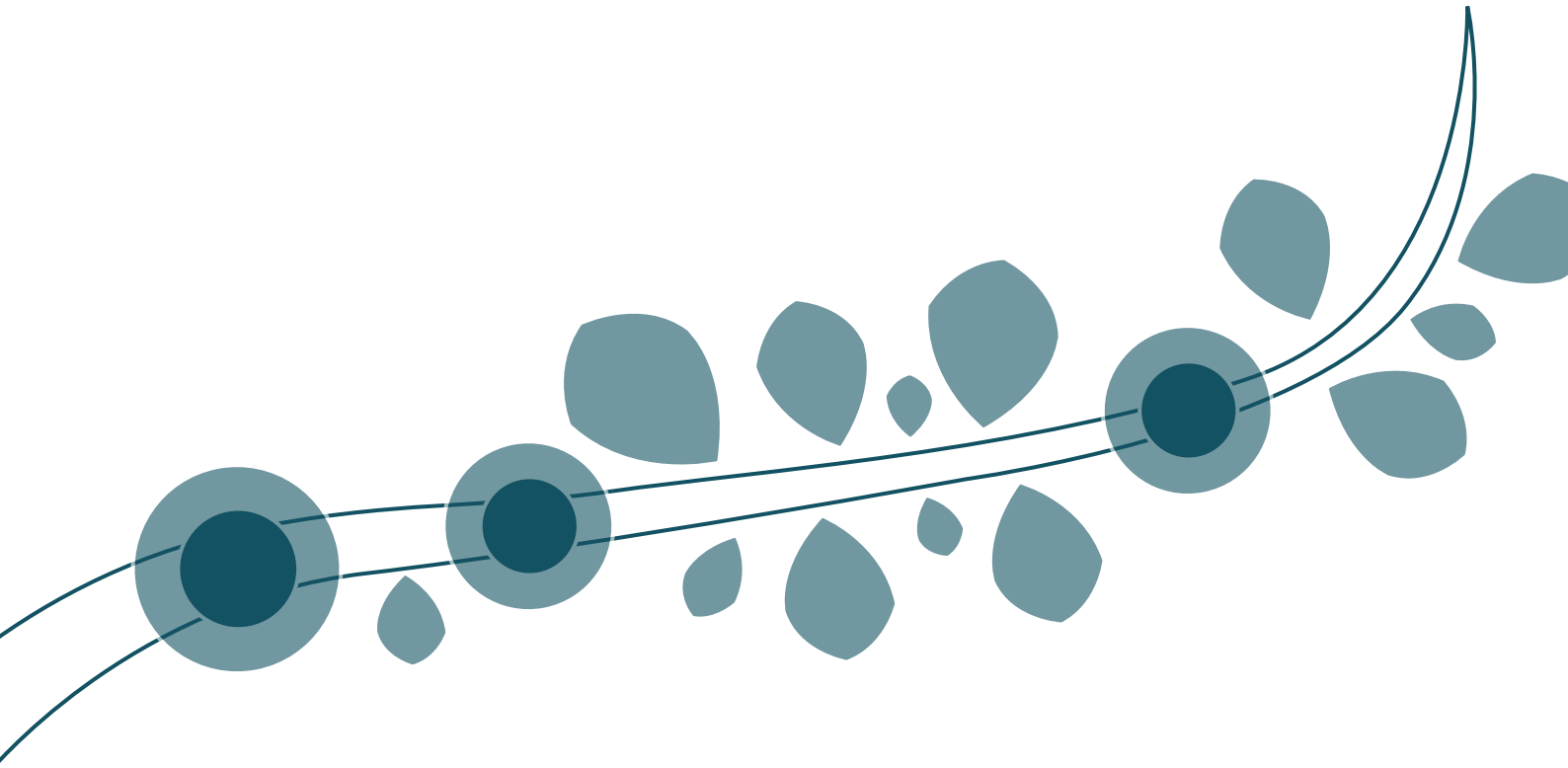
Avec le soutien de

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Fonds national d'aménagement et de développement du territoire

Sunta

Sommaire



{ 1 } Préambule

Cette Charte Cybersécurité de la Corse établit un socle commun visant à structurer l'écosystème corse dédié à la cybersécurité, articulé autour de la souveraineté numérique, d'un numérique de confiance et d'une coopération renforcée entre acteurs publics et privés.

Intégrée à la stratégie CyberCorsica définie par le livret N°12 du Schéma Directeur Territorial d'Aménagement Numérique de la Corse SMART ISULA, elle repose sur sept engagements thématiques et une gouvernance partagée.

{ 2 } Principes

La présente charte s'inscrit dans le prolongement des principes éthiques définis par la démarche SMART ISULA. Elle s'aligne aussi avec la charte de la Donnée et de l'intelligence artificielle définie dans le cadre de la création du service public de la donnée et de l'intelligence artificielle de la Corse.

Elle affirme la volonté de construire en Corse un espace numérique souverain, sécurisé et protecteur, fondé sur la confiance.

Elle constitue le socle fondateur de l'initiative collective CyberCorsica, portée par une gouvernance partagée entre les signataires.

En définissant un cadre commun de valeurs, d'engagements et de bonnes pratiques, elle veut fédérer l'ensemble des acteurs publics et privés de la cybersécurité en Corse.

Par ailleurs, elle formalise une démarche de marque territoriale, CyberCorsica, destinée à :

- Incarner les valeurs de la charte ;
- Déployer des actions de valorisation, d'information et de promotion ;
- Servir la stratégie cyber de la Corse au bénéfice du territoire et de ses habitants.

À l'échelle territoriale, globale et internationale, cette marque contribuera à mettre en lumière la dynamique des acteurs corses engagés dans la démarche.

Modalités d'adhésion et cadre juridique :

L'adhésion à cette charte repose sur une démarche volontaire. Elle ne se substitue en aucun cas aux dispositions légales et réglementaires en vigueur.

Les **conditions d'adhésion** sont les suivantes :

- Disposer d'un établissement public ou privé (y compris associatif) implanté en Corse ;
- Disposer d'au minimum un personnel basé en Corse ;
- Y exercer une activité effective.

L'adhésion à la charte est réservée aux personnalités morales.

Les signataires s'engagent à :

- Mettre en œuvre les principes et actions prévues par la charte, dans la limite de leurs moyens ;
- Partager les bonnes pratiques, mutualiser les ressources et collaborer activement pour renforcer la cybersécurité en Corse ;
- Promouvoir la marque CyberCorsica, participer à sa gouvernance et contribuer à son rayonnement par leur expertise.

Titre 1 : Engagement de compétences

Les signataires s'engagent à garantir un niveau d'excellence dans leur offre de services cyber, par :

- L'obtention et le maintien de certifications attestant de la qualité de leurs prestations ;
- Une veille active sur les évolutions du secteur, afin d'actualiser en continu leurs compétences ;
- La participation à des groupes de travail et des initiatives CyberCorsica dédiés à la valorisation des savoir-faire ;
- Le référencement de leurs compétences au sein d'un annuaire des acteurs CyberCorsica.

Ils s'engagent par ailleurs à appliquer et promouvoir les bonnes pratiques professionnelles en matière de cybersécurité (aspects techniques, juridiques, organisationnels, communication et protection des données), conformément aux règlementations en vigueur nationales (ANSSI et CNIL) et européennes.

Titre 2 : Engagement de sensibilisation et d'information

Les signataires contribuent à renforcer les actions d'animation et de sensibilisation autour de la Cyber en Corse en :

- Mettant leurs compétences au service d'initiatives CyberCorsica de sensibilisation auprès du grand public et des acteurs socio-économiques ;
- Participant à l'élaboration de programmes d'accompagnement et de modules pédagogiques qui pourront être partagés entre les acteurs ;
- Soutenant l'organisation d'événements Cyber s'inscrivant dans la dynamique CyberCorsica ;
- S'associant, le cas échéant, aux initiatives/dispositifs nationaux de sensibilisation (ANSSI, Cybermalveillance.gouv.fr), en cohérence avec les objectifs de la charte.

Titre 3 : Engagement de protection et de confiance

Les signataires promeuvent une culture de la confiance et de l'éthique dans les usages du numérique, en adéquation avec les valeurs de SMART ISULA et à celles liées à la stratégie DATA et IA de la Corse (charte de la donnée et de l'IA de la Corse).

À cette fin, ils s'engagent à :

- Promouvoir les principes d'éthique et de confiance dans les usages du numérique, en accord avec les valeurs portées par SMART ISULA.
- Respecter les bonnes pratiques professionnelles en termes de cybersécurité (techniques, juridiques, organisationnelles, communication, protection des données personnelles…).
- Respecter les questions liées au secret et à la confidentialité des informations, y compris dans le cadre du secret des affaires.
- Inciter à la prise en compte des problématiques Cyber (Cyber by Design) dans un système d'information, informatique ou de production, (sous-traitants, prestataires, clients, salariés…) dans le respect des principes de la Charte.
- Promouvoir auprès de la société insulaire les principes d'hygiène Cyber.
- Proposer des solutions pour lutter contre les atteintes aux données (notamment personnelles) et les phénomènes de désinformation.

Titre 4 : Engagement d'innovation et d'excellence cyber

Afin de participer à l'émergence d'un territoire d'excellence en cybersécurité, les signataires s'engagent à :

- Stimuler la recherche et développement (R&D) et les expérimentations dans le domaine cyber, en ciblant les spécificités insulaires ;
- Attirer et fidéliser les talents sur le territoire, en s'appuyant sur l'attractivité de la marque CyberCorsica ;
- Favoriser l'émergence d'une filière cyber corse, labellisée CyberCorsica, capable de rayonner en Méditerranée et à l'international ;
- Participer à la création d'un LabCyber territorial dédié à l'innovation, aux tests et à l'expérimentation.

Titre 5 : Engagement de cyberdéfense de la Corse

En cas de crise cyber affectant les intérêts de la Corse, les signataires s'engagent à :

- Mobiliser leurs compétences pour soutenir les actions de réponse ;
- Jouer un rôle de lanceur d'alerte en signalant tout risque identifié au collectif CyberCorsica et aux autorités compétentes ;
- Contribuer au déploiement de solutions de détection et de protection des infrastructures critiques ;
- Participer à un dispositif de veille et d'alerte coordonné, en lien avec le collectif CyberCorsica et les parties prenantes institutionnelles.

Titre 6 : Engagement en faveur du renforcement de l'écosystème

Les signataires œuvrent à la consolidation, la robustesse et la résilience de l'écosystème des acteurs cyber en Corse en :

- Coordonnant et clarifiant les mesures de soutien public pour en optimiser l'impact et l'efficacité ;
- Enrichissant l'offre de services cyber en Corse, en s'appuyant sur les principes de la charte ;
- Promouvant les formations académiques, continues et professionnelles dans le domaine ;
- Mettant à disposition un annuaire des prestataires cyber conformes à la charte ;
- Créant et alimentant un observatoire des risques cyber spécifiques à la Corse ;
- Assurant la promotion de la filière via la marque CyberCorsica.

Titre 7 : Dynamique collective CyberCorsica

Les signataires s'engagent à :

- Diffuser la charte et encourager de nouvelles adhésions ;
- Partager avec les autres membres toute information utile à l'amélioration de la connaissance et de la lutte contre les risques numériques ;
- Valoriser l'offre de services des adhérents ;
- Participer activement aux échanges au sein de la communauté ;
- Promouvoir la marque CyberCorsica et contribuer à la définition du futur Campus CyberCorsica.

Mise en œuvre de la gouvernance associée

La mise en œuvre de la charte repose sur une gouvernance définie par un règlement intérieur qui précise les modalités opérationnelles, notamment :

- La composition et le rôle du Comité d'orientation et de son bureau ;
- Les procédures d'adhésion, de suivi des signataires et de sortie de la charte ;
- Les documents formalisant l'engagement ;
- Les règles de fonctionnement du Comité d'orientation.

Vos projets

Vos contributions

Vos projets

Vos contributions

Vos projets

Vos contributions

Mentions légales

Charte CyberCorsica

Date de publication : janvier 2026

Éditeur : Cullettività di Corsica - Collectivité de Corse - 22, cours Grandval BP 215 - 20187 Aiacciu cedex ▪ Directeur de publication : le Président du Conseil exécutif de Corse ▪ Responsable d'édition : la Direction de la Transformation Numérique de la Corse ▪ Conception graphique : Benjamin Gour (Corsica Lab) ▪ Rédaction : l'équipe de la Direction de la Transformation Numérique avec le concours de l'entreprise SYNEOR.

Ce document est disponible en téléchargement sur le site https://ambizionedigitale.isula

SMART ISULA

Schéma Directeur Territorial
d'Aménagement Numérique de Corse

Charte CyberCorsica

CULLETTIVITÀ DI **CORSICA**
COLLECTIVITÉ DE **CORSE**

www.smart-isula.corsica

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

SMART ISULA

Schéma Directeur Territorial d'Aménagement Numérique de Corse

Règlement intérieur de la charte CyberCorsica

Sunta

Sommaire

{ 1 } Préambule

Dans un monde de plus en plus interconnecté, la cybersécurité est devenue une priorité essentielle pour protéger les données, les infrastructures, et la vie privée de chacun. En Corse, où l'équilibre entre modernité et traditions forge une identité unique, il est crucial de garantir un environnement numérique sécurisé et résilient.

La Charte Cybersécurité de la Corse « CyberCorsica » a pour vocation de rassembler l'ensemble des acteurs publics et privés autour de principes communs pour anticiper les risques, répondre efficacement aux menaces, et promouvoir une culture de la sécurité numérique. Elle repose sur une démarche collaborative et volontaire, affirmant que la cybersécurité n'est pas seulement une responsabilité technique, mais un engagement collectif.

Adhérer à cette Charte, c'est s'engager dans une dynamique de confiance mutuelle, de vigilance partagée, et de solidarité insulaire face aux défis du numérique. C'est aussi renforcer l'attractivité et la compétitivité de la Corse, en se dotant de pratiques exemplaires pour sécuriser ses réseaux et protéger ses acteurs économiques, sociaux, et institutionnels.

Ce document présente les étapes nécessaires pour rejoindre cette initiative. Il précise les modalités et engagements liés à l'adhésion, ainsi que les bénéfices attendus pour les signataires. Nous vous invitons à découvrir cette démarche et à participer activement à la construction d'un espace numérique corse plus sûr, résilient et innovant.

Le présent règlement intérieur a pour objet de préciser l'organisation entre les partenaires de la charte CyberCorsica et les processus associés.

Ce document est écrit par la Collectivité de Corse et précise les processus d'entrée et de sortie ainsi que les attendus pour les demandeurs et signataires de la Charte.

{ 2 } L'organisation et la comitologie

Comité d'orientation CyberCorsica.

Le **comité d'orientation CyberCorsica** réunit tous les signataires de la charte et les structures ayant droit (ANSSI, CNIL, Cybermalveillance…).

Il est l'instance de gouvernance de la dynamique CyberCorsica.

Ses recommandations sont prises de manière collégiale. Elles orientent la stratégie CyberCorsica et coordonnent la marque territoriale CyberCorsica.

Des collèges pourront être formés au sein du comité d'orientation, par exemple :

- Usagers publics et privés : entités privées et publiques, non prestataires informatiques ou numériques, qui s'inscrivent dans une démarche volontaire et vertueuse en cybersécurité.
- Prestataires : dans ce collège, sont attendus les prestataires informatiques et numériques ainsi que des entreprises proposant un service lié au numérique telles que cabinet d'avocats, assurances, banques ;
- Institutions investies : entités publiques susceptibles d'apporter un soutien financier à la filière et à la démarche CyberCorsica.
- Organismes de formation : entités privées ou publiques réalisant des opérations de sensibilisation et assurant des formations.

Le comité d'organisation fonctionne sur la base du consensus.

Bureau du comité d'orientation.

Le bureau du comité d'orientation est le groupe formé par les signataires de la charte sous l'égide de la Collectivité de Corse.

Il est constitué à l'origine par un représentant institutionnel de la Collectivité de Corse, un représentant de l'ANSSI, et un représentant des services de l'Etat en Corse.

Le bureau peut s'élargir à d'autres partenaires signataires de la charte qui souhaitent en faire partie au fil des adhésions.

La candidature de ces partenaires reste soumise à approbation des membres d'origine sus mentionnés.

Le bureau a la responsabilité du processus d'engagement dans la charte, notamment la rédaction des fiches de candidature. Il veille au respect des engagements des signataires.

Les membres du bureau s'engagent à respecter la confidentialité des informations qu'ils sont amenés à examiner lors de l'instruction des demandes.

Le bureau assure le suivi technique et l'application des décisions, orientations définies en comité d'orientation.

Le secrétariat du bureau et son animation sont assurés par les personnels de la Collectivité de Corse.

{ 3 } La candidature

Entités éligibles à l'adhésion.

L'engagement dans la dynamique CyberCorsica adresse toute entité publique ou privée ayant une activité en Corse et une représentation en Corse en lien avec la stratégie Cybersécurité de la Corse définie dans le livret du SDTAN de Corse SMART ISULA intitulé « stratégie cyber de la Corse : CyberCorsica).

Sont éligibles, des entités non domiciliées en Corse liées par des partenariats stratégiques en matière cyber à des entités basées en Corse et adhérentes à la charte.

Acte de candidature.

L'engagement dans la dynamique CyberCorsica passe par la signature formelle de la charte par une entité morale (la signature de la Charte étant dévolue à l'accord formel de la gouvernance de cette entité qui peut être publique ou privée).

Les demandes d'adhésion s'inscrivent dans une démarche volontaire et vertueuse, une volonté d'intelligence collective.

Demande de signature de la Charte

Chaque entité qui souhaite adhérer à la Charte et compter parmi les signataires devra adresser une demande motivée et appuyée de la validation formelle par la gouvernance de l'entité candidate. La demande doit être explicitement exprimée, une fiche de candidature est mise à disposition à cet effet.

Toute demande de signature de la charte CyberCorsica, est étudiée par le bureau et soumise aux adhérents.

Le bureau étudie les candidatures et formule un avis. Le bureau peut organiser un entretien avec certains candidats.

Les adhérents sont consultés et chaque candidature est validée sur la base d'un consensus défini en réunion.

Documents formalisant l'engagement dans la Charte

- Charte à signer.
- Courrier de confidentialité sur les informations transmises dans le cadre de la dynamique de la charte.
- Demande/validation des informations pour parution à l'annuaire CyberCorsica,
- Adoption du règlement intérieur.
- Délibération de la gouvernance du candidat à l'adhésion à la charte

Suivi du signataire

L'engagement est d'un an renouvelable par tacite reconduction.

Chaque année, un compte rendu d'activité est élaboré par le bureau, auquel chaque signataire peut faire valoir son engagement au sein du collectif et son respect de la charte.

Le signataire se rend disponible, du fait de son engagement dans la charte, pour participer à l'élaboration du compte rendu.

Sortie de la Charte

Tout signataire est libre de se désengager à tout moment en adressant un courrier électronique de désengagement au bureau, en précisant s'il le souhaite la motivation de ce retrait.

A la suite d'un changement de statuts, une entité, ne répondant plus aux critères de la charte tels que renseignés lors de la demande et de l'instruction, peut être radiée des signataires sur décision du bureau.

À la suite de manquements relevés dans les engagements d'un signataire, ce dernier peut être radié sur décision exprimée par le bureau et le comité d'orientation.

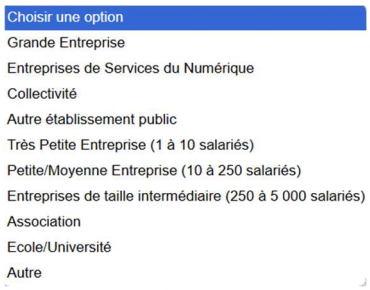
{ 4 } Le formulaire

Le formulaire de candidature est à renseigner sur le site Web (www.cybercorsica.isula/formulaire)

Les champs marqués d'un astérisque * sont obligatoires.

Informations de l'organisation candidate

- Nom organisation *
- Type *



- Secteur *
- Nombre de collaborateurs et collaboratrices *
- E-mail de contact public (adresse mail de contact qui sera affichée sur notre site internet)
- Adresse site web institutionnel*
- Code postal *
- Ville *
- Pays de résidence *
- Ajouter un logo *
- Présentation *

Informations du représentant signataire

- Nom *
- Prénom *
- Fonction *
- E-mail *
- Téléphone (au format international. Ex : +33) *

Informations du contact référent (si différent du représentant signataire)

- Nom
- Prénom
- Fonction
- E-mail
- Téléphone (au format international. Ex : +33)

Information complémentaire

- Veuillez sélectionner un pays de résidence dans la section « Informations de l'organisation candidate »

{ 5 } Le fonctionnement du comité d'orientation

Le comité d'orientation se réunit sur convocation du bureau et sur un ordre du jour défini.

Il se réunit à minima une fois par semestre.

Le compte rendu est assuré par le secrétariat du bureau.

Le comité d'orientation peut décider de réunions spécifiques selon le besoin.

Si collège il y a, les réunions d'un collège restent ouvertes à l'ensemble des membres du comité.

Le comité d'orientation est animé par le bureau, l'animation pouvant associer les membres du comité qui souhaitent y participer.

Son fonctionnement est collégial et ses propositions se décident de façon collégiale.

{ 6 } La mise à jour du présent règlement

Initiative de mise à jour

- La mise à jour du règlement intérieur peut être initiée par les membres du Bureau d'Orientation.
- Toute proposition de modification doit être rédigée de manière formelle, argumentée, et accompagnée des éléments de justification nécessaires.

Processus d'examen par le Bureau d'Orientation

- Les membres du Bureau d'Orientation examinent les propositions de mise à jour lors de leurs réunions ordinaires ou extraordinaires.
- Une fois validée par une majorité simple des membres du Bureau d'Orientation, la proposition est formalisée en projet de mise à jour.
- Le projet est communiqué au Comité d'Orientation au moins 15 jours avant la réunion où il sera soumis au vote.

Vote par le Comité d'Orientation

- Le projet de mise à jour est soumis au Comité d'Orientation lors d'une session ordinaire ou extraordinaire.
- Le Comité d'Orientation et le bureau se mettent d'accord par consensus pour :
  - Approuver le projet, auquel cas la mise à jour entre en vigueur immédiatement ou à une date spécifiée,
  - Rejeter le projet, auquel cas le règlement intérieur reste inchangé,
  - Demander des amendements, renvoyant ainsi le projet au Bureau d'Orientation pour révision.

Communication de la mise à jour

- Une fois approuvée, la mise à jour du règlement intérieur est communiquée à l'ensemble des membres sous forme écrite.
- Une version actualisée du règlement intérieur est mise à disposition sur les canaux officiels (site internet, circulaires, ou autres moyens appropriés).

Respect des principes fondamentaux

- Toute modification du règlement intérieur doit être conforme aux principes fondamentaux de la charte, aux statuts de l'organisation, et aux dispositions légales en vigueur.
- En cas de conflit, le Comité d'Orientation peut consulter un avis juridique pour garantir la conformité des modifications proposées.

SMART ISULA

Schéma Directeur Territorial
d'Aménagement Numérique de Corse

Règlement intérieur de la charte CyberCorsica

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

www.smart-isula.corsica