TAVITA CYBERSECURITY
GARDIEN CYBER DES TERRITOIRES

COLLECTIVITÉS TERRITORIALES

ACCOMPAGNEMENT CYBER SUR MESURE DES COLLECTIVITÉS

Anticipez, protégez, gouvernez votre cybersécurité pour une collectivité résiliente, conforme et souveraine — de la petite commune à l'intercommunalité.

LES COLLECTIVITÉS, UNE CIBLE DE CHOIX

État civil, fiscalité, action sociale, RH, eau, écoles : les collectivités gèrent des données sensibles et assurent des services essentiels. Elles sont devenues l'une des cibles privilégiées des cybercriminels : les bilans 2025 de l'ANSSI, de la CNIL et de Cybermalveillance.gouv.fr le confirment.

5 078
collectivités et administrations assistées par le 17Cyber en 2025, en hausse de 22 % sur un an
Source : Cybermalveillance.gouv.fr, rapport d'activité 2025 [1]

24 %
des 1 366 incidents traités par l'ANSSI en 2025 visent ministères et collectivités (2e secteur le plus touché)
Source : ANSSI, Panorama de la cybermenace 2025 [2]

128
compromissions par rançongiciel signalées à l'ANSSI en 2025, dont 11 % de collectivités territoriales
Source : ANSSI, Panorama de la cybermenace 2025 [2]

6 167
violations de données notifiées à la CNIL en 2025, un record (+9,5 % en un an, +50 % en trois ans)
Source : CNIL, rapport annuel 2025 [3]

Les Outre-mer ne sont pas épargnés : Collectivité Territoriale de Martinique (2023), Le Robert (2023), Collectivité Territoriale de Guadeloupe (2022), Mahina en Polynésie française (2024), Conseil départemental de La Réunion (2024) — toutes victimes de rançongiciels.

[1] Cybermalveillance.gouv.fr, *Rapport d'activité et état de la menace 2025* — cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2025 · [2] ANSSI, *Panorama de la cybermenace 2025*, CERTFR-2026-CTI-002 — cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025 · [3] CNIL, *Rapport annuel 2025* — cnil.fr/fr/rapport-annuel-2025 (montant des sanctions 2025 : même source).

SE METTRE EN CONFORMITÉ N'EST PLUS UNE OPTION

RGPD Mesures techniques et organisationnelles adaptées (art. 32), notification des violations à la CNIL sous **72 h**, désignation d'un DPO (art. 37).

NIS 2 Gestion des risques, suivi des événements de sécurité, plans de continuité, audits réguliers et notification des incidents majeurs pour les entités essentielles et importantes.

LPM Exigences renforcées de détection, de réaction et d'audit pour les services critiques (eau, énergie, transport, sécurité civile) et les opérateurs d'importance vitale.

CGCT Obligation de continuité du service public (art. L. 1111-1) : PCA/PRA, sauvegardes fiables et gestion de crise cyber deviennent incontournables.

SANCTIONS
486,8 M€ d'amendes prononcées par la CNIL en 2025 [3] ; sanctions NIS 2 et contrôles préfectoraux avec délais imposés.

CONFIANCE
Atteinte à l'image auprès des administrés, des autorités de tutelle et des partenaires.

FINANCEMENTS
Exclusion des programmes conditionnés à la conformité cyber (FEDER, ANCT, fonds ANSSI).

Choisir TAVITA CYBERSECURITY, c'est faire le choix d'un partenaire de confiance, expert, réactif et engagé pour la protection durable de votre système d'information.

NOTRE RÉPONSE AU VERSO →

UN ACCOMPAGNEMENT PERSONNALISÉ, CONSTRUIT AVEC VOUS

Chaque collectivité est unique par sa taille, ses ressources, son niveau de maturité et son exposition. TAVITA CYBERSECURITY refuse toute approche standardisée : après un diagnostic préalable, nous construisons un dispositif proportionné, modulaire et déployable par paliers, sur plusieurs exercices budgétaires si nécessaire.

ADAPTÉ À VOTRE NIVEAU DE MATURITÉ

Initiation

Sensibiliser élus et direction, poser les bases de la gouvernance SSI, sécuriser les fondamentaux (sauvegardes, MFA, segmentation), amorcer la conformité.

Consolidation

Formaliser la gouvernance (RSSI, comité SSI), professionnaliser la gestion des risques, bâtir les plans de crise, préparer les audits NIS 2 et LPM.

Montée en maturité

Référentiels avancés (ISO 27001, ANSSI), supervision continue (SOC, EDR, SIEM), risques tiers, exercices de crise de haut niveau.

DES MODULES À ACTIVER SELON VOS PRIORITÉS

1 — Audit et sécurisation du SI
Active Directory, Microsoft 365, pare-feu, EDR, réseau et Wi-Fi, sauvegardes, applications, scan web ; puis accompagnement à la remédiation.

2 — Audit organisationnel
Cartographie des processus, rôles, obligations réglementaires et niveau de maturité ; plan d'amélioration priorisé.

3 — Sensibilisation et formation
Élus, DGS, agents métiers, DSI, DPO : hygiène numérique, campagnes de phishing simulées, formation des techniciens.

4 — Gouvernance SSI et conformité
PSSI, charte informatique, analyse de risques, comité SSI, cartographie des exigences RGPD, NIS 2, LPM, RGS et plan de mise en conformité.

5 — Gestion de crise cyber
PCA/PRA, plan de réponse aux incidents, exercices sur table, escalade vers la direction et les autorités (ANSSI, CNIL, Préfecture).

6 — Supervision et maintien en condition de sécurité
SOC/EDR (Wazuh), journalisation, gestion des vulnérabilités et durcissement continu, avec reporting mensuel.

TROIS MODALITÉS D'INTERVENTION, COMBINABLES

RSSI externalisé

Pilotage SSI récurrent à temps partagé, conseil à la direction et aux élus, interface avec l'ANSSI et la CNIL.

Conseil stratégique ponctuel

Schéma directeur cyber, mise en conformité, volet sécurité de vos projets numériques et de mutualisation.

Intervention opérationnelle ciblée

Audit, remédiation, sensibilisation ou réponse à incident, en présentiel et en télémaintenance sécurisée.

VOTRE INTERLOCUTEUR

David TOUCHE — Gérant et consultant en cybersécurité

Architecte système, réseau et sécurité, ancien des forces armées : 23 ans au Ministère des Armées dans la sécurité des systèmes d'information et de communication, 28 ans d'expérience en SI dont 17 en cybersécurité. Master 2 Architecte système, réseau et sécurité, certifié ISO/IEC 27005 Risk Manager. Membre de la Cybersecurity Flying Squad Paris 2024 à Teahupo'o. Il intervient personnellement sur chaque mission, en présentiel et à distance.

Ils nous font déjà confiance : 6 collectivités accompagnées en Polynésie française et en Martinique, dont 5 contrats de RSSI externalisé · 57 projets d'audit et de sécurisation · 11 interventions après cyberattaque · 234 personnels formés.

SUR MESURE, SUR DEVIS

Un premier échange et un diagnostic de votre exposition suffisent pour bâtir une proposition adaptée à vos priorités et à votre budget.

contact@tavita-cybersecurity.com
+33 6 99 63 17 11 · +689 87 30 41 25
www.tavita-cybersecurity.com
Nous suivre : linktr.ee/TAVITACYBERSECURITY