

CYBERSÉCURITÉ DES FÉDÉRATIONS SPORTIVES FRANÇAISES

DOSSIER RÉALISÉ PAR LA TASK FORCE IA-SPORTS

NOTE D'ANALYSE · 2026 · MATRICE DE RISQUES ET RECOMMANDATIONS OPÉRATIONNELLES

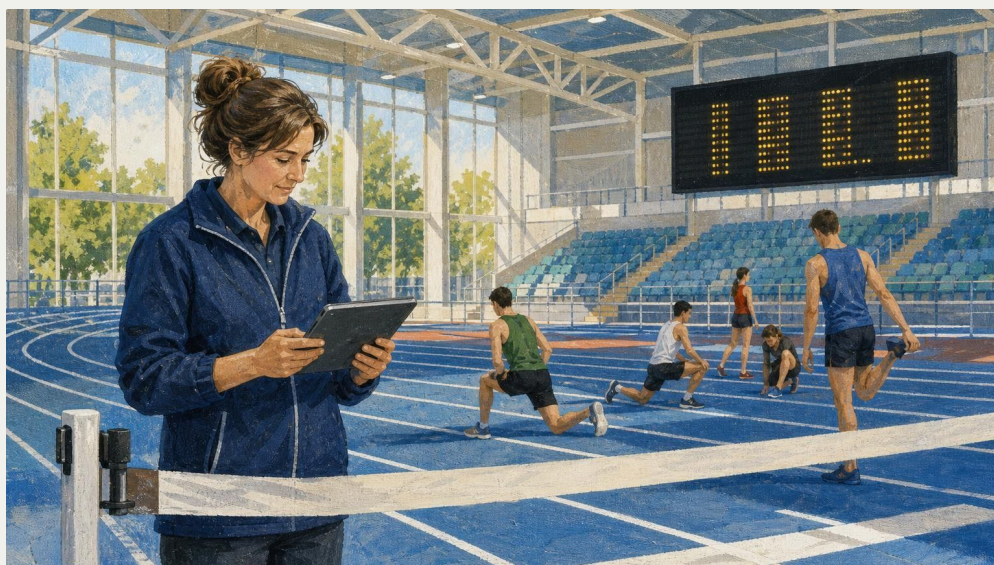


Fig. 1 Le sport fédéral repose désormais sur des systèmes numériques aussi critiques que ses terrains.

Matrice de risques et recommandations opérationnelles

Lecture intégrée des risques majeurs révélés par les attaques de 2025-2026 et des actions prioritaires, au regard des exigences de l'ANSSI, du CNOSF et du ministère des Sports.

SOMMAIRE

Une fragilité systémique	p. 02
Matrice de synthèse	p. 03
Les sept risques	p. 04
Gouvernance cyber	p. 11

Une fragilité systémique révélée par les attaques de 2025-2026

Les incidents survenus en 2025 et 2026 ne relèvent pas d'une série d'accidents isolés. Ils mettent en lumière une vulnérabilité structurelle du mouvement sportif fédéral, dont les fondations numériques ont été bâties par strates successives, souvent sans vision d'ensemble de la sécurité.

Les systèmes de gestion des licences, conçus pour certains il y a plus d'une décennie, coexistent avec des outils plus récents fournis par des prestataires hétérogènes. Cette mosaïque multiplie les interfaces, les comptes d'administration et les points d'entrée, tout en rendant difficile une maîtrise complète des flux de données.

À cette dette technique s'ajoute une dimension humaine et organisationnelle. La culture de cybersécurité reste peu diffusée, la gouvernance numérique est rarement formalisée et les dispositifs de réponse aux incidents font souvent défaut : lorsqu'une attaque survient, les fédérations improvisent.

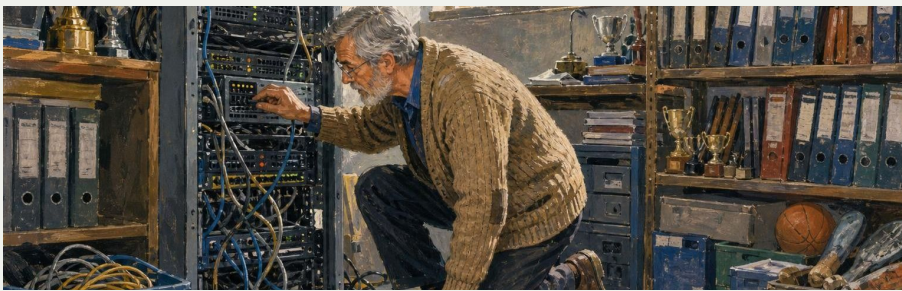


Fig. 2 Des infrastructures vieillissantes, héritées et rarement cartographiées.

Systèmes de licences vieillissants et dépendance de prestataires hétérogènes.

Culture de cybersécurité absente et gouvernance numérique peu formalisée.

Réponse aux incidents rarement préparée ni exercée.

Objet du document : structurer les risques, leurs impacts et les actions à engager, afin d'offrir aux dirigeants fédéraux une base de décision commune.

Matrice de synthèse : sept risques, probabilité et impact

Chaque risque est positionné selon sa probabilité et son impact, avec la mesure prioritaire qui lui répond.

Risque	Probabilité	Impact	Mesure prioritaire
Fuite des données des licenciés	Élevée (avérée)	Élevé	Cartographie RGPD, minimisation, chiffrement
Rançongiciel	Élevée	Élevé	Sauvegardes hors ligne testées, PCA cyber
Prestataires numériques	Élevée	Élevé	Clauses cyber, audits, tests d'intrusion
Données médicales et sensibles	Moyenne	Très élevé	Environnements isolés, double authentification
Identités des dirigeants et bénévoles	Élevée	Moyen à élevé	Formation, MFA, alerte interne
Sabotage des compétitions	Moyenne	Élevé	Systèmes de secours, tests de résilience
Atteinte à la réputation	Élevée	Élevé	Communication de crise coordonnée

Tableau 1 Matrice des risques cyber des fédérations sportives françaises.

Les évaluations sont qualitatives (élevée / moyenne) et constituent une appréciation indicative. Chaque fédération doit les ajuster à sa taille, à ses systèmes et à son exposition. Cinq risques sur sept cumulent une probabilité et un impact élevés : la priorité n'est donc pas de choisir un risque, mais d'organiser une réponse d'ensemble.

Risque 1 : compromission des données personnelles des licenciés

Un risque déjà matérialisé, au cœur de la relation entre fédération et pratiquants.

Ce risque n'est plus théorique : des fuites ont touché la gymnastique, l'athlétisme, le tennis de table, la randonnée et l'UNSS. Les bases de licenciés concentrent de nombreuses données, souvent conservées sans limite de durée et accessibles à de nombreux utilisateurs.

Les informations exposées comprennent l'identité, les coordonnées, les certificats médicaux et les documents administratifs. Leur combinaison permet l'usurpation d'identité et un hameçonnage crédible citant le club ou la licence de la victime.

Les impacts sont triples : sanctions possibles de la CNIL au titre du RGPD, perte de confiance des licenciés et des familles, et image durablement dégradée auprès des partenaires.

Recommandations

- Cartographier les traitements et identifier les responsables.
- Minimiser les données collectées et leur durée de conservation.
- Segmenter les accès selon les rôles, du siège au club.
- Auditer les prestataires qui hébergent ou traitent les données.
- Chiffrer et compartimenter le stockage.

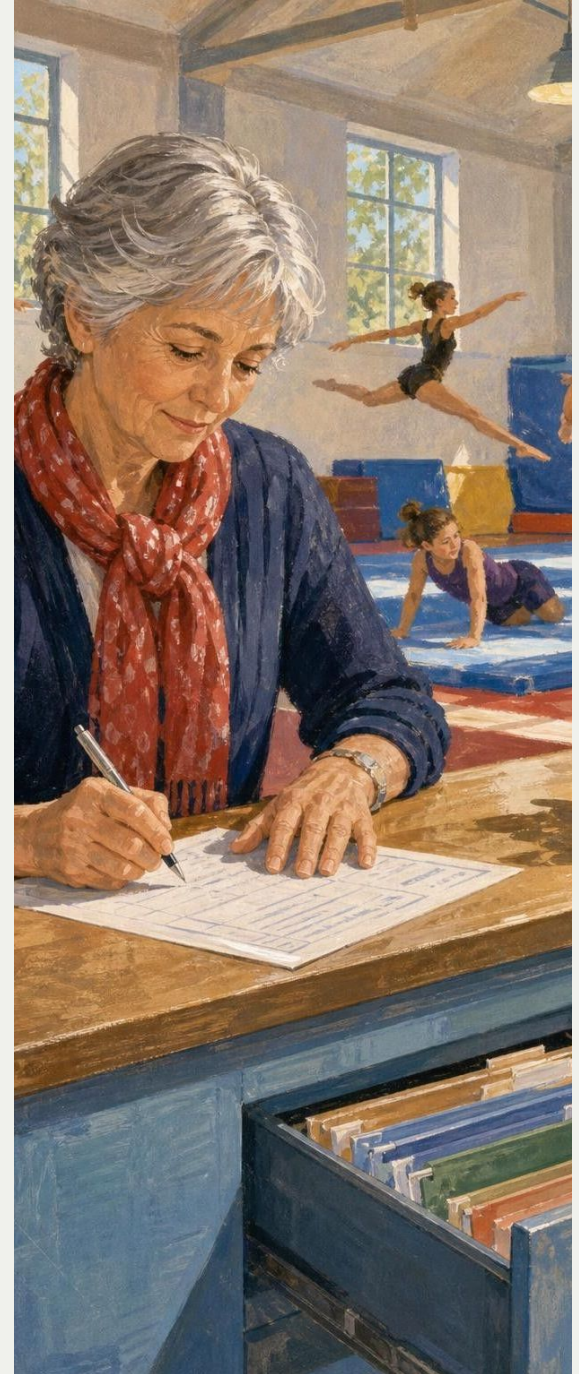


Fig. 3 Chaque inscription alimente une base dont la protection engage la fédération.

Risque 2 : rançongiciel paralysant les systèmes fédéraux

Des clubs professionnels et des fédérations européennes ont déjà été touchés ; le mouvement sportif français n'est pas à l'abri.

Un rançongiciel chiffre les serveurs et les postes, puis exige une rançon contre leur restitution, souvent assortie d'une menace de publication. Pour une fédération, l'effet est immédiat : licences bloquées, compétitions désorganisées et communication avec les clubs interrompue au moment où elle serait la plus nécessaire.

La réponse repose sur la capacité à fonctionner sans le système attaqué : des sauvegardes hors ligne réellement testées, une segmentation du réseau qui limite la propagation et des mises à jour automatisées. Ces mesures s'inscrivent dans un plan de continuité d'activité cyber, prévoyant une bascule vers un mode dégradé.

PLAN DE CONTINUITÉ D'ACTIVITÉ CYBER

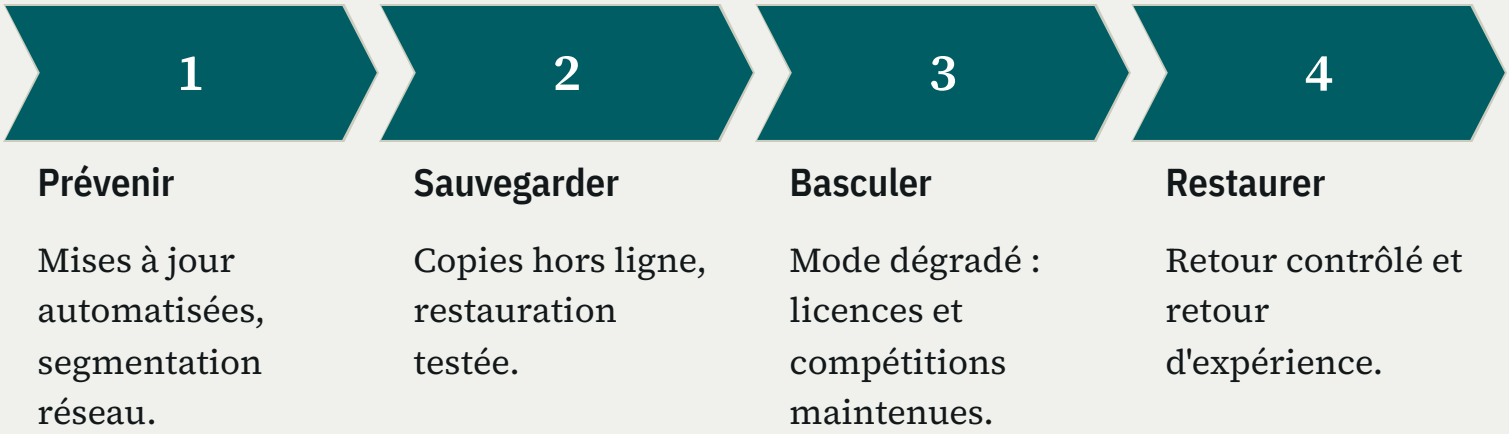


Fig. 4 Les quatre temps d'une continuité d'activité face au rançongiciel.

Le mode dégradé se prépare à froid

Listes de contacts imprimées, procédures papier de délivrance des licences, canal de communication de secours avec les clubs : ces éléments doivent exister avant l'incident et être exercés au moins une fois par an.

Risque 3 : prestataires numériques et écosystème technique

Les fédérations dépendent fortement de partenaires externes pour leurs licences, leurs intranets, leurs sites et leurs plateformes de compétition. Leur sécurité devient, de fait, celle de la fédération.

En 2026, la compromission d'un seul prestataire a exposé plusieurs fédérations à la fois. Cet effet de concentration est caractéristique des attaques par la chaîne d'approvisionnement : l'attaquant cible le maillon commun plutôt que chaque organisation.

Or les contrats en vigueur traitent rarement de sécurité : ni obligation de notification, ni droit d'audit, ni exigence de journalisation.

La maîtrise de ce risque passe par la relation contractuelle. La fédération doit pouvoir connaître, vérifier et contrôler ce que ses prestataires font de ses systèmes et de ses données, en particulier pour les services jugés critiques.

Les accès des prestataires doivent être nominatifs, limités dans le temps et révocables.

Exigences à intégrer

01 Clauses contractuelles de cybersécurité

Notification des incidents, responsabilités et réversibilité.

02 Audits et certification des prestataires critiques

Vérification indépendante du niveau de sécurité.

03 Contrôle des accès

Comptes nominatifs, droits minimaux, revue périodique.

04 Journaux, preuves de conformité, tests d'intrusion annuels

La confiance se démontre par des éléments tangibles.

Risque 4 : données médicales et informations sensibles

Les fédérations détiennent des informations parmi les plus protégées par le droit : dossiers médicaux, certificats, déclarations d'accident et données de mineurs. La probabilité de compromission est moyenne, mais l'impact est très élevé.

Leur valeur marchande et leur potentiel de nuisance en font des cibles de revente ou d'usage malveillant contre les athlètes : chantage, atteinte à la vie privée, exploitation d'une blessure ou d'un état de santé à des fins de pression.

Isoler et contrôler les accès

Les isoler du reste du système d'information dans des environnements dédiés, réserver les accès aux seuls personnels habilités et imposer une double authentification systématique réduit fortement la surface d'exposition.

Limiter la conservation

Ne pas conserver ce qui n'est plus utile : une durée de conservation limitée et la suppression automatique des documents obsolètes diminuent mécaniquement le

préjudice potentiel d'une fuite.

DONNÉES CIBLÉES

Dossiers médicaux et certificats d'aptitude.

Déclarations d'accident et suivis de blessure.

Données de mineurs : vigilance renforcée.

Mesures clés

- Environnements dédiés
- Accès restreints
- Double authentification
- Suppression automatique



Isoler les dossiers, maîtriser les accès.

Risque 5 : identités numériques des dirigeants et bénévoles

Le phishing ciblant les élus fédéraux et les responsables de clubs est en hausse.

Les dirigeants concentrent des pouvoirs de signature, des accès étendus et une visibilité publique qui facilitent l'usurpation. Un courriel imitant un président ou un trésorier suffit parfois à déclencher un virement.

Les bénévoles, souvent équipés d'outils personnels et peu formés, constituent un point d'entrée privilégié.

Les conséquences prennent trois formes principales : virements frauduleux, accès non autorisés aux systèmes fédéraux et communication détournée, lorsqu'un compte compromis diffuse de fausses informations aux clubs.

La protection des identités est une mesure peu coûteuse au regard des préjudices évités.

RECOMMANDATIONS



Formation obligatoire

Sensibilisation des dirigeants aux techniques d'hameçonnage et de fraude au président.



Authentification multifacteur

Activée sur la messagerie, les outils financiers et les plateformes fédérales.



Alerte interne

Un circuit simple pour signaler un message suspect et vérifier un ordre de virement.

UNE IDENTITÉ COMPROMISE SUFFIT À OUVRIR TOUTES LES PORTES DE LA FÉDÉRATION.

Risque 6 : perturbation ou sabotage des compétitions

Chronométrage, billetterie, diffusion et gestion des compétitions sont devenus des cibles à part entière.

La compétition est le moment où la fédération est la plus visible et la plus exposée. Un chronométrage altéré, une billetterie paralysée ou une diffusion interrompue suffisent à compromettre un événement et l'équité sportive elle-même.

Le risque s'accroît lors des événements à forte visibilité, qui attirent des attaquants en quête d'audience ou de revendication. La probabilité est jugée moyenne, mais l'impact est élevé, car l'incident se déroule en direct.

La réponse passe par la sécurisation des infrastructures critiques, des systèmes de secours capables de prendre le relais et des tests de résilience avant chaque événement majeur.

Elle exige enfin une coordination étroite avec les organisateurs locaux et les autorités publiques, pour que chacun connaisse son rôle avant l'incident.



Fig. 5 Le chronométrage électronique, point névralgique de l'équité sportive.

Risque 7 : réputation et confiance du public

Le risque réputationnel est la conséquence commune de tous les autres.

Il se joue moins dans l'incident que dans la manière d'y répondre.

Une fédération perçue comme négligente subit une baisse des licences, une défiance des clubs et la fragilisation de ses partenaires institutionnels. Ces effets durent bien après la résolution technique de l'incident.

À l'inverse, une réponse transparente et maîtrisée peut préserver, voire renforcer, la confiance. La crédibilité se reconstruit par les actes, démontrés publiquement.

Communiquer

Une communication de crise transparente et réactive, préparée en amont.

Coordonner

Avec la CNIL et l'ANSSI, et accompagner les licenciés concernés.

Démontrer

La mise en œuvre de mesures correctives robustes et vérifiables.

Accompagner les licenciés

Informers clairement les personnes concernées de la nature des données exposées, des risques encourus et des précautions à prendre est à la fois une obligation et le levier le plus direct pour maintenir la confiance.

La cybersécurité devient un impératif de gouvernance, plus seulement un sujet technique.

Vers une gouvernance cyber fédérale



Fig. 6 La sécurité numérique entre au comité directeur.

Structurer

Désigner un référent cybersécurité, réunir un comité numérique, formaliser une politique de sécurité et lui allouer un budget dédié.

Diffuser

Installer une culture de vigilance auprès des clubs et des bénévoles, premiers maillons de la chaîne.

Mutualiser

S'appuyer sur le CNOSF pour partager expertises, achats et standards communs, au bénéfice des fédérations les moins dotées.

Piloter

Réviser la matrice de risques chaque année et en rendre compte aux instances et aux partenaires publics.

Glossaire

RGPD	Règlement européen encadrant la protection des données personnelles.	Chiffrement	Transformation des données les rendant illisibles sans clé.
CNIL	Autorité française de protection des données, à notifier en cas de fuite.	Segmentation réseau	Cloisonnement du réseau pour limiter la propagation d'une attaque.
ANSSI	Agence nationale de la sécurité des systèmes d'information.	Sauvegarde hors ligne	Copie des données déconnectée du réseau, hors d'atteinte des attaquants.
CNOSF	Comité national olympique et sportif français.	PCA	Plan de continuité d'activité : maintenir les services essentiels pendant une crise.
UNSS	Union nationale du sport scolaire.	Mode dégradé	Fonctionnement minimal et manuel lorsque les systèmes sont indisponibles.
Rançongiciel	Logiciel malveillant qui bloque ou chiffre les données contre rançon.	Test d'intrusion	Attaque simulée pour détecter les failles avant les pirates.
Phishing	Hameçonnage : message frauduleux visant à voler identifiants ou données.	Journaux d'activité	Traces des connexions et actions, utiles pour détecter et enquêter.
Authentification multifacteur	Double authentification : plusieurs preuves d'identité pour se connecter.	Prestataire critique	Fournisseur dont la défaillance perturberait l'activité de la fédération.