# Résumé des points abordés RSI Etablissements de sport
# 27-29 novembre 2019

**Participants :**
Guillaume VINCIGUERRA (Creps Bordeaux), Sylvain DANGIN (Creps Ile de France), Brice GILLION (Creps Nancy), Jean-Marc BATALLER(Creps Montpellier), Jean-Michel BOLLIET (Creps PACA), Anthony CHENARD (Creps Pays de Loire), Jean-Pascal MOUSSET(Creps Poitiers), Maxime RIBERY (Creps Reims), Jean-Louis CANN (Creps Réunion), Jean-Michel EON (Creps Vallon-Pont-d'Arc), Yannick VIGIER (Creps Toulouse), Paul DE SA (Creps Vichy), Didier COLPART(Creps Wattignies), Bruno THERY (CNSNMM-ENSM), Jean-Claude GERARD (ENVSN), Marc GERY(IFCE), Benoît ZEDET(ANS), Benoît NOQUET (DS), Brigitte ETCHEGARAY (DSI)

**Sécurité SI : Fabien Malbranque**
Dans chaque rencontre, il est prévu autant que possible, d'aborder les sujets essentiels de sécurisation des systèmes d'information afin de permettre avec les RSI, information et sensibilisation sur des thématiques d'actualités, partage de bonnes pratiques et retour d'expériences. Trois points étaient à l'ordre du jour des sujets Sécurité abordé par le FSSI adjoint des ministères sociaux.
Dans ce cadre, et pour commencer ci-dessous deux vidéos de sensibilisation à la sécurité des systèmes d'information diffusées en séance :
Le premier plutôt à destination d'informaticiens : https://www.youtube.com/watch?v=sI9mxu8Y_Nk
Le second plutôt à destination des utilisateurs : https://www.youtube.com/watch?v=I5jZWXbFP5c

**Actualités ramsonware :** retour d'expériences global sur l'incident de l'hôpital de Rouen
La situation telle que médiatisée sur l'attaque dont a été victime le CHU de Rouen est une nouvelle fois l'occasion de rappeler qu'en situation de crise il convient de garder son sang-froid.
La position est claire, partager pour ne pas subir ! Mais ce type d'incident nécessite de la prudence sur les communications de par l'impact que cela peut avoir sur le traitement de l'incident lui-même mais aussi parce que la judiciarisation de son traitement interdit la communication d'éléments pour ne pas faire obstruction.

Concernant les éléments de posture à mettre en œuvre pour se prémunir, ce sont irrémédiablement les 42 règles d'hygiène avec une attention particulière sur :

- La maitrise de points d'accès externes, messagerie à distance, accès à distance type RDP, accès VPN
- La maitrise des accès internet, filtrage d'URL, et probablement interdiction des accès aux messageries personnelles
- La maitrise de la sécurité des flux de messagerie, antispam antivirus….
- La protection de vos annuaires avec la réduction drastique du nombre de comptes ayant des privilèges élevés et la surveillance de l'usage de ces derniers.
- La réduction au stricts besoins des utilisateurs des droits sur les espaces de stockage des fichiers.
- La déconnexion des systèmes de sauvegarde en dehors des plages d'utilisation de ces derniers.
- Il est rappelé que le compte utilisé pour réaliser des actions d'administration ne doit en aucun cas avoir accès à internet et à la messagerie

**Concernant l'obligation d'homologuer les systèmes d'information** : voir la présentation jointe

Le référentiel général de sécurité (RGS), c'est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. L'arrêté du Premier ministre du 10 juin 2015 a prorogé le délai de mise en œuvre du référentiel au 1er juillet 2016.

Il convient d'homologuer l'ensemble de vos applications au sens RGS du terme à défaut, tous les systèmes doivent être homologués au sens de la PSSI-MCA. Il est bien évident que tout ne peut être fait en une seule fois mais l'engagement des structures pour homologuer tous les nouveaux projets est indispensable pour faire progresser le niveau de sécurité de vos SI.
Le dossier de sécurité est relativement simple à constituer, conformément à la réglementation : https://www.ssi.gouv.fr/uploads/2014/06/Lhomologation-en-neuf-etapes-simples-Document-types.pdf

L'homologation est un processus vertueux qui permet d'identifier les risques afin de mettre en place des plans d'actions pour réduire ces derniers. Le comité d'homologation, présidé par le directeur de la structure (AQSSI) permet à ce dernier au regard des risques brutes identifiés, des risques résiduels après traitement d'avoir conscience des risques auxquels le système ou le l'application reste exposé.
Le processus d'homologation sur des processus clefs (Analyse de risques, mise en place des plans d'actions, contrôle de l'état de sécurité (Audits, tests d'intrusion).
Comme je l'ai dit en séance, le processus d'homologation est un processus vertueux qui permet d'intégrer les problématiques de sécurité au démarrage du projet.

**Office365 :** voir le document d'homologation sécurité produit par le HFDS/SSI
Vous trouverez le document d'homologation relatif à Office365 qui a été introduit en séance et qui présente une analyse détaillée des risques, et dont il est nécessaire de prendre connaissance dans le cadre des éventuels changements effectués par certains établissements.

**Data and co : Pierre Vercauteren**
Une présentation sur le sujet Data a permis l'utilisation de l'outil collaboratif Klaxoon pour un partage immédiat utilisable dans des contextes variés d'ateliers (post-it, réponse à un questionnaire, partage d'idées, nuage de mots, quizz, classement etc…), outil pouvant supporter une méthode d'animation vivante et concrète. L'outil est convivial et peut être utilisé sur place ou avec des correspondants à distance.
On imagine bien l'usage d'un outil numérique de ce type dans le cadre d'un brainstorming sur un sujet nouveau ou d'une assemblée à plus grande échelle pour participer à un questionnaire et disposer de nombreuses réponses rapidement analysées avec un résultat restituable de façon automatique et immédiatement affichable à tous grâce à l'outil.
Il est testable gratuitement, mais pour en disposer de façon pérenne il nécessite l'acquisition de licences. A ce stade, la DSI en fait l'expérimentation et des présentations pour information dans le cadre de plusieurs réseaux ou groupes de travail pour faire mieux connaître ces possibles méthodes et outils d'animation.
S'agissant de la présentation Data, elle a permis de promouvoir l'importance des données au sein de nos organisations, tout en rappelant les problématiques qui y sont liées, et les réflexions qui peuvent être menées pour les partager et les valoriser, et en rappelant les piliers des 5V pour les données : Volume, Vélocité, Variété, Véracité et Valeur.

**Projet INSEP/PSQS et plateformes : Eric Labouchet**
Plusieurs sujets abordés concernant les actualités de l'INSEP et du PSQS, notamment des travaux d'audit et de mise en sécurité des éléments des plateformes mises en œuvre par l'INSEP.

PSQS :
Voici les évolutions fonctionnelles réalisées en 2019

1- Général
   a. Page synthétique des informations du sportif
   b. Export pdf d'un sportif
   c. Notion de groupes utilisables par les services

   d. Modification des interfaces de gestion des groupes
   e. Notion de pôle affichable dans les applications mobiles
   f. Export des groupes fédéraux dans les services web
   g. Notion de structure principale
   h. Création d'un espace dédié à la gestion des pièces d'identité
   i. Mensurations des sportifs
2- Préinscription
   a. Choix des sportifs
   b. Modification de la gestion des clubs
3- Mise en liste
   a. Modification de la gestion des sportifs maintenus
   b. Ajout des notions de dates de débuts de performance et de date de parution de l'arrêté
   c. Mise en place de l'intégration de l'ensemble des sportifs (tous les listé et tous les sportifs appartenant à une structure du PPF)
   d. Notion de structure principale
   e. Intégration de la saisie de trois pièces d'identité dans la pré-inscription de la mise en liste
   f. Mise en place de la signature électronique des conventions
   g. Gestion des messages pour les fédérations
   h. Gestion des clubs plus efficace
   i. Gestion des non classés dans les services web
4- Cartographie
   a. Amélioration des performances des services web
   b. Modification suite à la demande de ANS
   c. Module direct dans le PSQS
   d. Statistiques
5- Facturation
   a. Vérification de l'intégrité des données (date de fin)
6- Fédérations
   a. Mise en place de la notion de cadre de groupe fédéral
7- Module ANS
   a. Modification de la gestion des épreuves de références
   b. Associations des disciplines de chronos aux sports du PSQS
   c. Affichages de données synthétique (Date d'évaluation, classement des colonnes)
   d. Amélioration du processus d'import des données de Chronos
8- Module sportifs listés
   a. Modification des statistiques
   b. Exports des données statistiques
9- Application mobile
   a. Modification des feuilles d'appel
10- Module bourses
   a. Définition et mise en place du module
   b. Mise en place de la signature électronique
11- Module MGI
   a. Outil de gestion des missions

Des points d'attention ont été passés à propos de la sécurisation du dispositif PSQS INSEP et de sa mise en conformité RGPD, notamment dans le cadre de conventions passées avec les établissements.

Une réunion sera organisée sur le sujet avec le prestataire assurant le rôle de DPD au sein de l'INSEP en présence de la DS.

**Projet INSEP Data :**

Concernant l'appel d'offre il s'agit de mettre en place un Athlète Monitoring Systèm (AMS) afin de fédérer l'ensemble des datas autours de la performance avec les datas INSEP et grand INSEP. Le but est de structurer et architecturer nos datas (recherche, perf, suivi longitudinal..etc..).
A ce titre plusieurs sociétés ont répondu (My Coach/ Fusion / SAP / PLAYSHARP).
Nous avons bâti la demande pour une mise en œuvre avec deux périodes de maquettage.

- Déploiement sur l'infra INSEP (Vitry)
- Liaison et connexion avec les BDD externes (développement de 6 API).
- Démonstration de la génération des rapports synthétiques prenant en compte les datas provenant de 6 sources externes.

**Plateforme de gestion des centres de formation :**

- Il est prévu la mise en place d'une plateforme de gestion des centres de formations en relation avec l'évolution de la loi.
  Il s'agit de la société AXES via son logiciel agate :
  http://www.axess-solutions-formation.fr/agate-logiciel-gestion-centres-formation/
  En cours de déploiement pour l'INSEP, la FD de HAND et sur début 2020 la FD de Tennis.
  Travail sur ces 6 derniers mois à son interconnexion avec notre plateforme de FOAD afin de disposer d'une offre globale prenant en compte du catalogue de formation jusqu'à l'intégration du paiement dans les SI des FD (incluant le paiement en ligne).
  Une présentation via le grand INSEP sera probablement organisée.
  La partie un peu délicate est l'intégration sur la fédération d'identité avec les FD.

**Sécurisation de la plateforme INSEP :**

- Concernant la partie SI et RSSI INSEP Vitry
  Déploiement du bastion Wallix (gestion des accès à privilège) :
  https://www.wallix.com/bastion-privileged-access-management/
  Déploiement de la solution Commvault sur la partie sauvegarde
  PSSI en relation avec la PSSI du Ministère des affaires sociales
  Déploiement d'une pré-production complète
  Mise en conformité RGPD avec DPO externalisé
  Audit Intrusion (1) qui sera suivi d'un deuxième audit ciblé PSQS et FOAD avant la fin de l'année.
  Déploiement d'un PRA sur un deuxième data center (actif début 2020)

- Renforcement sur la partie matériel :

Ce, afin d'accueillir les potentiels PPR (AO projet de recherche), et il y a déjà un projet recherche ciblé ANS / INSEP en cours sur la médaillabilité.

**Présentation de l'ANS : Benoît Zedet** – voir présentations jointes

L'ANS présente son organisation et ses objectifs, ainsi que le projet Data Hub : constituant un des projets SI phares de l'ANS lancé en cette fin d'année 2019, il s'agit de construire une plateforme et une offre de service pour accueillir et rassembler les données de la performance sportive. Il est nécessaire d'identifier l'existant et le prévisionnel, les besoins fonctionnels et techniques à couvrir pour répondre à l'ensemble des organisations qui peuvent envisager de participer. Un recensement des données sera organisé dans les établissements de sport en 2020 en vue de dresser une cartographie. Toutes les suggestions sur le sujet sont les bienvenues, notamment les cas d'usage sont à répertorier et à consolider dans le cadre de cette phase de démarrage du projet.

**Projet Tir à l'arc et vidéos : société Inowys** – voir plaquette

Le dispositif vidéo pour le tir à l'arc mis en place au sein du CREPS Bordeaux est présenté dans le stade par la société Inowys.

La solution InoPerf a été conçue pour faciliter l'intégration de la vidéo dans les entrainements quotidiens des athlètes. Elle a été conçue pour permettre une mise en œuvre suivant les besoins de la discipline : choix du type de caméra (fixe, déplaçable, HD, …) , de méthode de diffusion (TV fixe ou amovible, vidéoprojecteur,…). Avec cette solution, plus aucune perte de temps pour optimiser les performances de vos athlètes grâce à la vidéo.

**Boîtiers BOA et RIE : Jean-François Escobosa**

Il est confirmé l'intérêt de disposer de boîtier à la fois pour analyser et auditer les flux et éventuellement y découvrir des anomalies (sollicitations techniques intempestives, Wsus, antivirus, ou autres, etc…) et corrections à apporter au fonctionnement réseau, et pour optimiser et prioriser les applications utilisées. L'ENVSN et le Creps de Bourges ont pu bénéficier de cette offre mise en place par le Noc RIE et y trouver un retour sur un fonctionnement nominal. Ce dispositif est bien entendu à surveiller et à exploiter afin notamment d'y intégrer les nouveaux services ou utilisations des agents. Les retours côté DDI suite à une mise en place massive montrent que la résolution des problèmes de performances ne passe pas nécessairement par l'augmentation des débits des liens. Par ailleurs, la PFAI RIE a été améliorée à l'automne 2019 pour permettre une meilleure efficience de l'accès à l'Internet qui devrait montrer des améliorations au niveau des temps de réponse. Il est à étudier la manière dont les établissements intéressés pourraient faire l'acquisition d'un tel système. La grille tarifaire correspondante est jointe.

**Accès distants Carinae : Brigitte Etchegaray**

Pour rappel, les accès distants Carinae permettent aux agents de travailler à distance ou en mobilité et d'accéder à leurs ressources et outils de travail mis à disposition sur le réseau RIE. Il s'agit d'un VPN sécurisé utilisé par l'ensemble des ministères sociaux, services déconcentrés, agences et établissements utilisant le réseau RIE. Il est mis à disposition notamment pour tous les agents qui ont des journées de télétravail. Cet accès va être très utilisé pendant la période de grève qui s'annonce. La DSI s'est chargée de renforcer sa disponibilité par des équipements et des mises à jour logicielles, et le retour d'expérience de la période récemment passée s'avère bon. Dans tous les cas, cet outil largement utilisé dorénavant est suivi de près.

Le dispositif nécessite préalablement la mise à disposition d'un certificat pour le compte créé dans l'annuaire AD SD et d'un kit à installer sur le poste de travail. Pour que le réseau soit accessible, il faut que l'antivirus soit à jour et actif. Dans le cas où il ne l'est pas, les utilisateurs peuvent lancer manuellement la mise à jour de l'antivirus sur Internet et recommencer la connexion.

Une nouvelle version 15 est à tester/installer pour remplacer notamment la version 13 (date en 2018) qui n'est plus supportée et la version 14 (date été 2019). Le module sera transmis aux pilotes qui se sont proposés. Il est rappelé l'usage de la documentation lorsque des problèmes sont rencontrés : copie d'écran, tracert et ping sur les services qui seraient non accessibles, à transmettre pour analyse des premiers cas à Brigitte Etchegaray pour vérifier la faisabilité pour l'accès aux ressources serveurs tout d'abord. Ensuite, si cela est OK, un ticket sera à faire pour demander l'ouverture de flux en précisant l'adresse IP/DNS en vue d'atteindre ces serveurs en mode accès distant Carinae, si ce n'est pas déjà le cas actuellement.

**Projet DS organisation : Benoît Noquet**

L'organigramme joint de la DS suite à sa réorganisation est présenté. A savoir notamment que le bureau chargé de la Tutelle des établissements est DS2A. Cette réorganisation prend en compte la répartition des missions avec l'ANS récemment créée. Et à prévoir le rattachement des structures au ministère de l'éducation nationale avec des conventionnements en cours par exemple côté gestion RH ou côté SI notamment pour les applications mises en œuvre par les ministères sociaux.

**Cocwinelle : introduction Jean-Michel Bolliet**

Pour la reprise des données Cocwinelle, il est partagé l'idée que ce sont essentiellement les données tiers qui sont à reprendre dans le dispositif GFI, ce qu'il est possible de faire via le logiciel.
A voir de plus comment Cocwinelle peut continuer à être utilisé pour disposer des données des années de gestion précédentes.

**RGPD et ateliers : Benjamin Seymour** – voir présentation

Différentes thématiques ont été présentées :

- La protection des données du site Internet : le sujet d'information et de limitation des cookies est concerné notamment.
- Le Wi-Fi mis à disposition du public : ce sujet a fait l'objet de multiples échanges, car la gestion de l'accueil s'étant avérée lourde, par exemple pour les stagiaires d'un ou plusieurs jours, les pratiques d'attribution de codes pour y accéder sont variées. Plusieurs modes peuvent être mis en place selon le type de population géré. Une charte d'utilisation peut être mise en commun pour essayer de partager sur le sujet.
- Les Checklist sécurité des SI : c'est un préalable pour identifier ce qui est déjà fait et à faire dans ce domaine, les SI étant toujours à protéger
- La responsabilité et la co-responsabilité : il s'agit d'identifier avec ses prestataires ce qui est à faire pour être en conformité pour tous les traitements à données personnelles utilisant des SI
- Outil Data Legal Drive : référentiels logiciels – un atelier spécifique est à prévoir afin de partager la saisie des référentiels entre les différents SI. Il n'a pas pu être mené faute de temps Pour cela, le tableau d'identification des SI mis à jour pourra être partagé.

**SI Formation : Jean-Marc Bataller –** (**document en attente**)

Le logiciel de formation élaboré au Creps Montpellier est présenté directement à partir du système lui-même et sur la plupart des fonctions qu'il couvre. Déjà utilisé à Creps Montpellier, ce logiciel est désormais en fonctionnement à Creps Ile de France avec un retour positif sur son fonctionnement et sa prise en mains, ainsi que sur le nombre de formations et de stagiaires déjà gérés avec l'application. Il apparaît que la gestion semble facilitée par un tel outil qui permet de stocker et de gérer les inscriptions, les dossiers en cours d'élaboration, leur paiement et leur suivi. Des évolutions sont en cours notamment pour la gestion des plannings des formations. D'autres déploiements sont prévus pour 2020. Il est nécessaire de mettre en place une gouvernance partagée du projet avec les établissements concernés, afin de mettre des priorités sur les corrections ou évolutions à mettre en œuvre. Il est également nécessaire que le logiciel soit en conformité RGPD et homologué au niveau sécurité. Une date est à convenir pour partager sur ces différents sujets. Des tutoriels ont été mis en place pour faciliter la formation aux fonctions du logiciel. Une documentation est attendue pour diffusion.

**Tchap : Thibault Leblanc -**

Un point est fait sur les évolutions de Tchap et les mises à jour en cours. L'interface Web sera améliorée pour disposer de nouveaux services.
Le Tchap est une messagerie instantanée sécurisée et mise au point par l'Etat. Elle permet l'échange rapide via smartphone ou PC entre collègues ou avec des partenaires connectés. Ce dispositif est ouvert à l'extérieur et permet des échanges sur un ou plusieurs salons privés où les partenaires peuvent être invités. Ce dispositif est notamment largement déployé et utilisé au sein de la Police et de la Gendarmerie pour des échanges professionnels et de partages. Des salons publics mis à disposition de tous permettent d'échanger et de contribuer sur toute sorte de thématiques. Tout agent s'il le souhaite peut se connecter à Tchap en déclarant son adresse de messagerie professionnelle et créer son salon pour faire participer d'autres collègues connectés ou partenaires invités.

**Bitlocker : François Poupard** – présentation jointe

Une présentation jointe permet de faire le point et retour d'expériences sur l'installation du logiciel de chiffrement Bit Locker en cours de déploiement sur les portables au sein des ministères sociaux. Ce logiciel est préconisé et recommandé pour améliorer la sécurisation et la confidentialité des données des postes de travail mobiles. Celle-ci présente les objectifs, une synthèse du produit et de sa mise en œuvre, et les paramètres GPO liés à mettre en place.

Deux ou trois établissements ont déjà mis en place cet outil sur les portables ; il est partagé avec eux, le fait que son utilisation est transparente pour l'utilisateur, que l'installation ne pose pas de problème particulier si on respecte les pré-requis et bonnes pratiques sur le sujet.

**Offres interministérielles : Brigitte Etchegaray**

Au-delà de la webconférence webex mise à disposition pour permettre des échanges (et que nous utilisons pour l'intervention de prestataires en mode sécurisé), il existe l'outil interministériel basé sur le produit libre jitsi. Il permet des échanges en interne RIE et avec des partenaires extérieurs et est très simple d'utilisation : https://webconf.numerique.gouv.fr

Il suffit d'y ouvrir un salon sur le réseau RIE et de transmettre l'URL aux destinataires. L'outil permet de visualiser les participants comme dans une visioconférence ou de présenter un document à l'écran, selon les besoins. A noter que cet outil répond aux contraintes d'homologation de sécurité émises par les différents FSSI des ministères. Utile de remonter les éventuelles difficultés que vous pourriez rencontrer notamment s'il y a des problèmes de performance.

**Bilan/Conclusions : Brigitte Etchegaray**

Retour sur le regroupement : le programme a été volontairement dense, et pour certains RSI, des sujets ont manqué de temps pour permettre leur approfondissement. Les attentes sont diverses selon les participants. Chacun aura pu probablement y trouver des thématiques intéressantes ou à creuser.

Certains au sein du réseau sont plus intéressés par des échanges sur des problématiques très techniques (réseau, wifi, bitlocker, W10, Vmware, etc…). D'autres selon leur positionnement au sein de leur direction portent plus ou également leur attention sur les SI choisis et mis en œuvre au sein de leur structure. Dans tous les cas, les thèmes à couvrir par les RSI sont variés.

Il est important qu'ils puissent apporter leur avis et contribution vis-à-vis de leur direction, afin de porter et soutenir la mise en place du numérique et des outils transverses liés aux postes de travail au sein de leur structure avec les meilleures pratiques SI et de sécurité. Ces rencontres favorisent largement les discussions et partages au sein du réseau et permettent d'approfondir des questions ou points spécifiques dans le cadre des retours d'expériences des collègues. Elles doivent également permettre la production de bonnes pratiques, favoriser le partage de SI et leur mise au commun pour permettre une évolution et une sécurisation des établissements dans le domaine stratégique du numérique.

**Prochain point** : en webconférence avant les congés de décembre