<u>Note de synthèse et de propositions option systèmes d'information et de communication</u> :

Métropole de Soigny Le 10 septembre 2025

A l'attention de Mme la Directrice Générale des Services

<u>Objet</u> : Mise en application de NIS2

La directive européenne NIS2 (Network and Information Security) est désormais à mettre en application à l'échelle de la France à travers la loi « Résilience des infrastructures critiques et renforcement de la cybersécurité ».
Dans ce contexte, notre collectivité est concernée puisqu'elle fait partie des 15000 entités jugées « essentielles », avec son lot de nouvelles obligations, mais aussi une plus grande capacité à être accompagnée. Je vous propose dans cette note de présenter dans un premier temps les grandes lignes de cette directive et quels sont les enjeux pour la collectivité, rendant son application incontournable. Dans un second temps, je souhaite vous mettre en évidence les leviers sur lesquels nous devons nous appuyer et les actions prioritaires que nous devons mettre en œuvre, avec notamment l'échéance des élections municipales 2026 en ligne de mire, comme temps critique face aux risques de cyberattaques.

A) Pourquoi mettre en œuvre NIS2 ? Car les risques sont réels et car nous en avons désormais le devoir et un cadre renforcé pour :

(1) Nos obligations en matière de cybersécurité

La directive NIS2 peut être vue comme un dispositif qui concernerait avant tout les entreprises européennes qui ont besoin de mieux protéger leurs activités critiques et leur savoir-faire, ainsi que les établissements à haut niveau de sécurité, notamment par la gestion de données de santé ou scientifiques. Mais les collectivités ont également été considérées dans cette loi renforçant les règles en matière de cybersécurité, cela a été confirmé par la commission résilience du Sénat. Et cela s'explique essentiellement par le degré de risque : les villes et communautés de communes sont régulièrement attaquées et nombre d'incidents ont été constatés (144 en 2024, deux tiers des incidents relevés par les collectivités). Nous avons donc obligation légale de sécuriser notre système d'information en tant qu'entité essentielle.
Certaines des obligations portées par NIS2 ne sont pas vraiment nouvelles et les collectivités, généralement proactives quand elles disposent d'une direction des systèmes d'information, ont déjà appliqué une partie d'entre elles. Nous pouvons notamment mentionner la nécessité d'une gestion des risques établie (idéalement en s'appuyant sur le cadre normé de l'ANSSI : la méthode EBIOS). Nous avons aussi obligation à mettre en œuvre un dispositif de sauvegarde robuste et étanche, ainsi qu'un plan de reprise d'activité (PRA) à l'échelle de notre SI.
Ce qui est particulièrement renforcé dans la demande des pouvoirs publics, c'est la nécessité de reporting et d'alerte quand des incidents sont détectés. Il est demandé de reporter immédiatement à l'ANSSI tout incident susceptible de mettre en péril notre SI.

Nous devons donc renforcer notre dispositif de surveillance, y compris pour ce qui concerne les systèmes gérés directement par nos fournisseurs (par exemples les solutions en Saas-Software as a Services, que nous n'hébergeons et ne gérons pas). Toute la difficulté réside donc dans le fait que notre surveillance est répartie et doit pourtant être la plus rapide possible (Les incidents critiques dans l'heure par exemple). Enfin, concernant les fournisseurs, la directive a permis d'expliciter leur obligation à se conformer aux normes de sécurité européennes et françaises, au-delà du RGPD (Règlement de Gestion des données personnelles) qui était déjà applicable depuis près de 10 ans. De ce point de vue, nous devons donc répercuter nos obligations de cybersurveillance vers nos fournisseurs. Et c'est notamment à ce titre que NIS2 est une réelle opportunité pour notre collectivité, cela nous apporte un cadre supplémentaire pour déléguer la gestion de la sécurité vers toutes les parties prenantes.

(2) Principaux risques et enjeux pour la Métropole

Nous avons été touchés par une attaque par déni de service fin 2023. Il s'agit d'un des principaux modes opératoires de la part des organisations malveillantes. Mais l'impact est moins sévère (Indisponibilité du service sans le corrompre) que d'autres formes d'attaques. La plus connue (car elle a touché plusieurs entreprises, CHU et même des collectivités ces dernières années) est probablement l'attaque par rançongiciel, avec le risque d'impact direct, comme le vol de données ou l'obligation de payer une somme conséquente. L'hameçonnage est une autre forme de vol de données en général, en proposant des liens et formulaire frauduleux à nos agents notamment, via les messageries professionnelles ou personnelles. L'utilisation des failles logicielles est aussi exploitée et les collectivités sont souvent prises pour cibles quand elles détiennent des versions peu mises à jour de certains logiciels. La bureautique est un grand facteur de risque, car il peut permettre la détection de failles et des techniques d'hameçonnage. Elle favorise aussi une nouvelle forme d'attaque, également très présente via les appels téléphoniques et les réseaux sociaux : il s'agit de l'hameçonnage social consistant à manipuler un utilisateur pour lui soutirer des informations (par exemple un mot de passe en se faisant passer pour un technicien de support). Toutes ces techniques ont pour principal effet le vol de données et l'introduction de données voire de codes altérés. C'est le risque de voir des données personnelles, financières ou sensibles être utilisées, tout comme voir certains de nos services arrêtés et vérolés. L'impact est d'autant plus élevé concernant nos services vers les usagers : portails famille, état civil, portails aux associations, etc. Car cela peut nuire à l'image de la métropole et bloquer certains services. Et en cette période pré-électorale, je pense que le risque peut être très élevé concernant nos médias de communication (le site web) tout comme notre dispositif de gestion des élections.
D'un point de vue retours d'expérience d'autres collectivités, les sites web sont bien souvent la première cible pour les cyberattaques. Il paraît donc très pertinent de mettre en place un dispositif de cybersécurité renforcé avec les attentes de NIS2, sans attendre concernant les mesures de protections les plus faisables.
Nous pourrions par exemple profiter du mois prochain pour porter le sujet haut et fort, car il s'agit du « mois de la cybersécurité » à l'échelle nationale.

Nous venons en tout cas de voir l'étendue des risques pour la métropole et ce que la directive NIS2 nous demande d'appliquer en tant qu'entité essentielle.
Cela peut paraître particulièrement contraignant, même si le renforcement de notre sécurité est incontournable au regard des risques. Mais cette démarche présente aussi des avantages qu'il nous faut saisir au bond, avec de nouveaux soutiens et l'occasion de capitaliser sur les expériences récentes (la nôtre en particulier), d'autant plus que de

nouvelles méthodes de cyberattaques pourraient arriver en s'appuyant sur l'IA générative. Il est donc question de robustesse (réagir aux attaques et être « armé » face au risque) tout autant que résilience (se préparer à l'incertain). Dans la seconde partie, je vais vous exposer les leviers qui s'offrent à nous pour utiliser NIS2 à bon escient, et les actions clés que je souhaite mettre en œuvre, dont certaines très rapidement.

B) NIS2 peut être une opportunité pour mobiliser et se renforcer dans notre démarche d'un numérique résilient

(1) Les leviers qui s'offrent à nous en cette fin 2025

L'avantage que la loi Résilience nous apporte tout d'abord, c'est de mettre les collectivités au cœur des préoccupations en matière de cybersurveillance. Cela offre une légitimité à tout un ensemble de leviers sur lesquels la métropole va pouvoir s'appuyer. D'abord l'ANSSI est un interlocuteur expert encore plus disponible, et pas uniquement sur le plan de la méthode et des normes (EBIOS, RGS). Il s'agit d'un partenaire de notre surveillance des incidents, pouvant nous accompagner plus opérationnellement. Il devient stratégique pour nous (avec le concours de notre RSSI) de nouer une relation régulière avec l'ANSSI. Nous devrions pouvoir également nous appuyer sur la CSIRT de notre territoire, pour traiter nos incidents critiques, ou nous aider dans nos actions de formation et sensibilisation. Il faut donc voir ces entités comme des soutiens d'expertise et d'analyse pour notre surveillance, cela renforçant notre robustesse et notre résilience.
Nous pouvons également utiliser les réseaux de soutiens entre collectivités dans des niveaux stratégiques (France Urbaine et les interconnectés) pour porter la voix des collectivités auprès de l'Etat ou du secteur de la cybersécurité, ou des niveaux plus opérationnels (Cité + par exemple) pour recueillir des retours d'expérience variés. Il sera enfin utile de s'appuyer sur les retours de la CNIL afin de compléter la veille technique et ajuster notre perception des risques majeurs.
Ensuite, il faut regarder les fonds d'aide financière, car les collectivités sont encore plus légitimes à revendiquer un soutien à l'innovation en matière de cybersécurité. Les fonds européen FEDER et français France Relance sont encore actifs en 2025 et 2026.
Ce dernier met l'accent sur l'aide à la transition numérique depuis déjà longtemps. Il peut y avoir aussi une opportunité à étudier via le fonds européen FSE+, car la cybersécurité est un secteur du numérique stratégique, mais qui requiert des compétences très spécifiques qui ne sont pas évidentes à acquérir pour nos agents. La mise en œuvre d'une cybersécurité renforcée passe aussi par une transformation de certains de nos postes.
En interne, nous avons aussi la possibilité de nous appuyer sur la mise en lumière des risques de cyber attaque. C'est l'occasion de sensibiliser nos élus davantage, ceux en charge du numérique mais pas que. Car le risque est sur tous les métiers. Auprès de nos agents par ailleurs, nous pouvons utiliser l'expérience acquise par la précédente attaque pour sensibiliser à un surcroît de vigilance, et en profiter pour mieux faire comprendre les nouvelles directives. A un niveau plus stratégique, la cybersécurité est un argument pouvant légitimer certains chantiers techniques nécessaires à la collectivité mais parfois jugés trop techniques par nos élus. C'est notamment le cas de la transition vers le Cloud souverain. Car la question de la sécurité et de la souveraineté des données devient particulièrement critique et peut apporter son lot de décisions incohérentes, pour des questions souvent financières. Avoir une telle orientation dans les choix d'infrastructures peut aider à mieux considérer les enjeux de sécurité et de souveraineté auprès des décideurs.
Du point de vue des projets le levier que nous apporte NIS2 est de porter un enjeu de rationalisation. Il devient indispensable de gérer 100 % de son parc matériel avec des

outils d'inventaire et de gestion du cycle de vie (sortie des PC par exemple). Et l'urbanisation du SI et une meilleure gestion de l'obsolescence et des dépendances prennent une toute autre dimension, avec l'enjeu de devoir mieux contrôler les risques d'intrusion. Il est très probable que ce travail de rationalisation puisse avoir un effet simplificateur : décommissionner l'obsolescent non essentiel, avec réduction de certains coûts de fonctionnement. L'argument de l'obligation de sécurité nous permet de sensibiliser à l'enjeu de qualité de notre SI, tout comme il peut nous aider à justifier la lutte contre les « Shadow IT », ces dispositifs numériques non maîtrisés par notre direction des SI et potentiellement non surveillés, donc à fort risque. L'ensemble le plus actuel est l'usage de l'IA générative. C'est actuellement un véritable « Shadow IT » non maîtrisé, où des agents peuvent parfois utiliser chat GPT pour manipuler des données sensibles sans le moindre contrôle. La sécurité est donc un argument fort pour tenter de mieux réguler ce nouvel usage. En définitive, un SI rationalisé et dont les usages sont maîtrisés est plus sécurisé, et donc plus résilient.

(2) Le plan d'action pour une métropole cyber résiliente

En m'appuyant sur les leviers que je viens d'exposer et sur les attentes réglementaires de la directive NIS2, je propose un plan d'action suivant cinq axes clés et dont l'importance clé est d'en faire un projet à part entière, avec une gouvernance dédiée. Nous pourrons voir que ces actions justifient un projet allant au-delà d'une problématique technique. Il s'agit d'un projet de transition, nécessitant la contribution des élus, de la direction générale en particulier.

La première action clé que nous pouvons démarrer rapidement consiste à réaliser un diagnostic de la précédente cyberattaque. Cela doit nous permettre de mettre en évidence les faiblesses de notre organisation pour pointer les principaux chantiers de mise en sécurité et de sensibilisation en interne. Je souhaite proposer au RSSI de piloter cette action avec la contribution d'un expert de l'ANSSI idéalement. Cette analyse est un prérequis aux deux actions suivantes qui concernent la mise en sécurité de notre SI et la sensibilisation de nos élus comme de nos agents ou partenaires.

La deuxième action clé est à pilote par notre chef de projet cybersécurité, en lien étroit avec notre RSSI et notre DPO. Il s'agit de la mise en œuvre du nouveau plan de sécurité (PSSI) de la métropole avec une revue de celui-ci en conformité avec NIS2.

Ce plan doit contenir une cartographie des fonctions et projets critiques ou hautement critiques d'une part. L'objectif sera d'accompagner les services concernés de façon différenciée. D'autre part, il faut initier ou mettre à jour la matrice de risque de cybersécurité selon la méthodologie EBIOS, puis mettre en place une solution de détection / alerte, avec un dispositif de surveillance supervisée. Cela doit permettre d'anticiper, détecter et reporter rapidement les incidents liés à des faits d'agents humains ou automatisés.

Les plans de reprise d'activité sont à collecter par ailleurs, auprès des différents projets numériques afin de vérifier leur niveau de conformité. Cette action plus longue à mettre en œuvre est à étaler en fonction de la criticité des projets. Il devient également indispensable d'avoir un plan de continuité d'activité (PCA) pour les services numériques critiques a minima, et pour le SI plus globalement. La gestion des postes de travail, du réseau, des centres de données et des applicatifs doivent bénéficier de consignes en cas de cyberattaque. Enfin le chef de projet pourra initier ou mettre à jour un clausier sécurité SI avec pour objectif de le diffuser à l'ensemble des chefs de projet numérique de la collectivité. Les dernières normes devront compléter ce que les RGPD et RGS demandent déjà.

La troisième action clé a pour objectif d'accompagner le changement, en mettant en œuvre un plan de sensibilisation et de formation auprès des parties prenantes. Cela

concerne tous les agents, mais aussi les élus et les fournisseurs, à travers nos actions de sourcing ou de gestion courante des projets. Quelques thématiques sont particulièrement importantes : la vigilance au quotidien évidemment, dans l'usage de son PC ou de sa messagerie, ou encore du téléphone.
Mais aussi les risques liés aux usages de l'IA et d'autres formes de « Shadow IT » (les outils de transfert par exemple).
Quelques outils peuvent être utile pour ce faire, en matière de sensibilisation : une note de service argumentée, une participation en Codir auprès de différents métiers, des contenus marquants sur l'écran quand il est en veille, ou à côté des imprimantes. Et puis réaliser des tests de vigilance a un gros avantage.
Envoyer par exemple des courriels piégeux permet de sensibiliser les agents et repérer les cas à risque. Le mois d'octobre peut nous permettre de lancer certaines de ces actions. Sur les deux actions précédentes, nous pouvons identifier qu'il nous faudrait a minima deux profils pour assister notre chef de projet. Un profil analyste et formateur et un profil technicien superviseur.
La quatrième action est plus stratégique et consiste à mettre en place un dispositif de gouvernance.
C'est à la fois de cartographier les organisations de soutien (ANSSI, CSIRT, etc.) et les leviers de financement possible. Afin de mettre en place les relais et lancer des projets financés si possible. En interne, il s'agit de mettre en œuvre un projet avec une instance de gouvernance incluant a minima un élu référent, un membre du Codir de la direction générale, la DSI, le RSSI e le DPO. Idéalement la contribution de directions métiers clés est un avantage. Ce projet doit permettre de piloter les actions précédentes, mais aussi de décider de projets d'envergure ou d'orientations pour les projets de transformation.
Enfin, la cinquième action consiste justement à instruire des projets de rationalisation. Plusieurs axes sont envisageables et la contribution de l'équipe sécurité a pour but d'apporter des règles de conduite et des recommandations. Nous avons notamment évoqué quelques types de projet : mise en Cloud, inventaire d'obsolescence ou dépendance, IA généralisée.
Le but est aussi de servir d'observatoire des transitions numériques, du point de vue de la cybersécurité et des risques associés.

En conclusion, le travail à faire en matière de cybersécurité est conséquent. Il faut mettre en œuvre tout un projet de mise en conformité NIS2 et de sensibilisation à 360° (Agents, élus, fournisseurs).
Mais c'est inévitable et nécessaire. Car au-delà du cadre réglementaire, le risque est réel et l'impact est important pour une métropole de notre envergure, qui plus est à 6 mois des élections municipales. Nous pourrions même aller plus loin, et sensibiliser et accompagner nos citoyens. Car le risque est désormais partout. La cybercriminalité touche les réseaux sociaux (l'Europe pense à contrôler les messageries tellement le risque est élevé) et tous les usages quotidiens. La métropole, avec ce projet, peut déjà monter qu'elle est exemplaire.