astee
L'association des professionnels
de l'eau et des déchets

La cybersécurité, un enjeu majeur dans les domaines de l'eau et de l'assainissement

Édition janvier 2025

Guide d'application

Ce guide a été réalisé par le groupe de travail « Cybersécurité »
rattaché à la Commission Eau potable de l'Astee

astee.org

Création graphique : Christelle Charlier

ISBN : 978-2-490604-17-3 9782490604173

Préambule

La cybersécurité constitue désormais un réel enjeu en raison de la digitalisation croissante des métiers de l'eau et de l'assainissement, ce qui accroît la vulnérabilité des installations.

Celle-ci va continuer de se développer dans deux domaines principaux :

- La gestion des installations qui ont vu se multiplier les capteurs, les automates, la transmission de données, les accès à distance et le pilotage centralisé.
- La gestion des informations, qu'elles soient techniques ou qu'elles concernent des données personnelles.

Ces données deviennent indispensables pour améliorer la performance du service, mieux connaître et anticiper les besoins et les contraintes de fonctionnement. En gestion publique ou déléguée, certaines particularités du secteur de l'eau peuvent par ailleurs complexifier l'organisation : diversité des rôles et responsabilités entre collectivités et exploitants, coactivité entre plusieurs types d'acteurs qui exploitent les infrastructures de l'eau, besoins d'échange d'informations…

Tout cela génère de nouveaux risques contre lesquels les collectivités doivent se prémunir avec un objectif fondamental : maintenir le service aux abonnés en garantissant la disponibilité, l'intégrité et la confidentialité.

Il convient donc de sécuriser le fonctionnement des installations et les systèmes d'information en prenant en compte des risques multiples : rançonnage, atteinte à la réputation au travers de la publication de fausses informations, indisponibilité des outils numériques, détournement de fonds au travers des fonctionnalités de paiement à distance… Dans le cas des installations de traitement d'eau, des cyberattaques permettant d'agir sur leurs consignes de pilotage peuvent avoir des conséquences directes dans le monde physique : perturbation de l'alimentation en eau potable de la population, pollution du milieu naturel, endommagement des ouvrages, modification des procédés des usines, etc.

En 2022, une nouvelle directive Européenne (NIS2) a été publiée. Elle étend très largement le périmètre des entités qui seront concernées par la réglementation de sécurisation vis-à-vis du risque cyber. Les secteurs de l'alimentation en eau potable et de l'assainissement sont explicitement pris en compte et les collectivités et administrations seront concernées.

Dans ce contexte, l'Astee a souhaité constituer un groupe de travail sur le sujet de la cybersécurité avec pour objectif de mettre à disposition des collectivités un ensemble de documents décrivant les enjeux et les règles de bonnes pratiques (dans le domaine industriel spécifiquement) adaptées aux réseaux d'eau potable et d'assainissement. Les collectivités et les exploitants devront par ailleurs veiller à protéger leur informatique de gestion (facturation, base abonnés, …).

Ce guide a donc pour ambition de permettre aux collectivités d'atteindre un haut niveau de protection face à ces nouvelles menaces.

L'Astee

L'Astee est l'association française des professionnels de l'eau et des déchets.

Reconnue d'utilité publique depuis 1905, elle est constituée de plus de 4 000 membres, personnes morales et physiques, professionnels de l'eau (eau potable, assainissement, gestion écologique des ressources en eaux et des milieux aquatiques) ainsi que des déchets et de la propreté urbaine. L'Astee a pour vocation la mutualisation des connaissances, des pratiques et des savoir-faire, et d'en faciliter l'accès au bénéfice de chacun. Elle est également sollicitée pour consolider des avis ou des recommandations aux pouvoirs publics.

Depuis 1905, l'Astee a su s'adapter aux évolutions de nos métiers et de leur environnement, tout en restant fidèle aux valeurs qui en font la force, dont en premier lieu le respect de la diversité qui la compose et la capacité à construire des consensus scientifiques et techniques. Elle est un carrefour de réflexions, de rencontres, d'échanges et d'informations ouvert à l'ensemble des acteurs publics et privés. Elle promeut des solutions concrètes au bénéfice du développement durable des services publics de l'environnement, par l'élaboration de doctrines collectives sur les meilleures pratiques, par l'accompagnement du progrès et des innovations, par le partage des retours d'expérience et la mutualisation des compétences, au bénéfice de la performance. L'Astee assure le rôle de point focal et de relais des grandes organisations internationales (IWA, ISWA, CEOCOR) et européennes (EWA), et travaille en partenariat avec de nombreuses associations (Partenariat français pour l'eau, AITF, ATTF, FNCCR, Académie de l'eau, SHF, AFEID, etc...).

Les membres du Groupe de travail cybersécurité de l'Astee

Co-pilotes

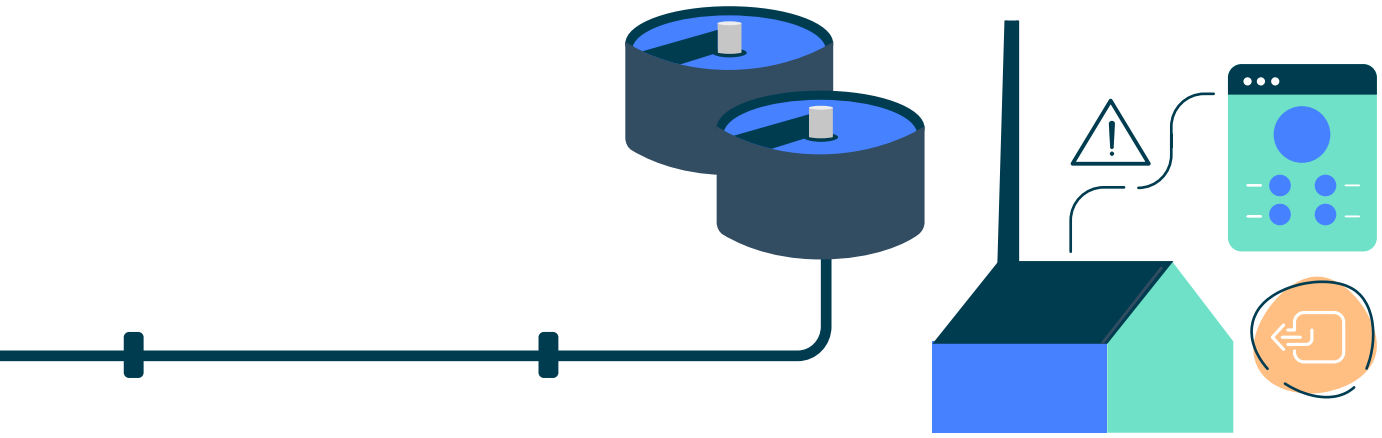
FOOTE	Alexander	Akandu Conseil
PICHARD	Thierry	Antea Group – IRH Ingénieur Conseil
RIVALLAN	Joël	Président Section Ouest Pays de Loire de l'Astee

Rédacteurs du guide

DEPREY	Maxime	Purecontrol
FILLAT	Éric	Mission d'Assistance à la Gestion de l'Eau et de l'Assainissement de la Gironde
HELFENSTEIN	Paul	Saur
LE MOUEL	Mikaël	Eau Du Morbihan
LOLMEDE	Philippe	Agglomération du Grand Cognac
MANCEAU	Patrick	Syndicat départemental d'alimentation en eau potable des Côtes d'Armor
MIRAULT	Frédéric	Suez
NICAISE	Vincent	Stormshield

Membres du groupe de travail

ALBOUY	Guillaume	Eau du Bassin Rennais
BARBET	Philippe	Agglomération Beziers-Méditerrannée
CHAPERON	Fabrice	La Croix Environnement
COURCIER	Jean-Paul	Veolia
DE LAVERGNOLLE	Emmanuel	Sedif
DEGUSSEME	François	Collectivité d'Agglomération du Saint Quentinois
DESLANDES	Vincent	STGS
FAYON	Sébastien	Sedif
GONZALO	David	SMDE24
GUERIN	Laeticia	INRAE
GUIGUEN	Fabienne	Agence technique départementale de l'eau 53
LAFFORGUE	Michel	Suez
LIRON	Maud	AFNOR
MARTIN	Aurélien	Eau de Paris
MEDJAHED	Mehalia	Xylem
MICHAUX	Bernard	Compagnie Intercommunale Liegeoise des Eaux
NGUYEN	Bruno	W-Smart
PERRIN	Nicolas	Grenoble Alpes Métropole
PHILIPPON	Victor	Xylem
RENARD	Jean-Luc	Sturno
SOUDARISSANANE	Mouthou	Xylem



Sommaire

P.06
1. La réglementation

P.08
2. Le référentiel cybersécurité Astee

P.37
3. Glossaire

P.40
4. Proposition de classement des collectivités

1. La réglementation

À l'heure actuelle, la réglementation relative à la cybersécurité s'applique très partiellement et uniquement dans le domaine de l'alimentation en eau potable.

Les textes majeurs sont constitués d'une part au niveau français par la loi de programmation militaire (LPM) et d'autre part, au niveau de la réglementation européenne par la directive « Network and information system security », dite directive NIS1, transposée en droit français en 2016. Cela concerne environ 300 opérateurs de services essentiels, dont certains dans le domaine de l'alimentation en eau potable. Ces opérateurs dits « d'importance vitale » ont été désignés par des arrêtés ministériels, toutefois non publiés.

L'Agence nationale de sécurité des systèmes d'information (ANSSI), rattachée au Premier Ministre, définit les exigences de sécurité pour les opérateurs d'importance vitale (OIV) et les contrôles. Pour l'ensemble des autres opérateurs, aucune réglementation ne s'applique.

La directive NIS2, entrée en vigueur en octobre 2022, élargit son périmètre à 18 secteurs d'activité (dont l'alimentation en eau potable, l'assainissement et les déchets) et devrait être plus prescriptive que la précédente. Plusieurs dizaines de milliers d'entités devraient désormais être concernées et être obligées de mettre en œuvre cette réglementation relative à la cybersécurité. Des collectivités et des administrations pourront également être concernées.

La directive NIS2 définit les concepts d'entité essentielle (EE) et d'entité importante (EI). La différence est liée à l'activité et la taille de la structure et permet de proportionner les exigences applicables à ces entités.

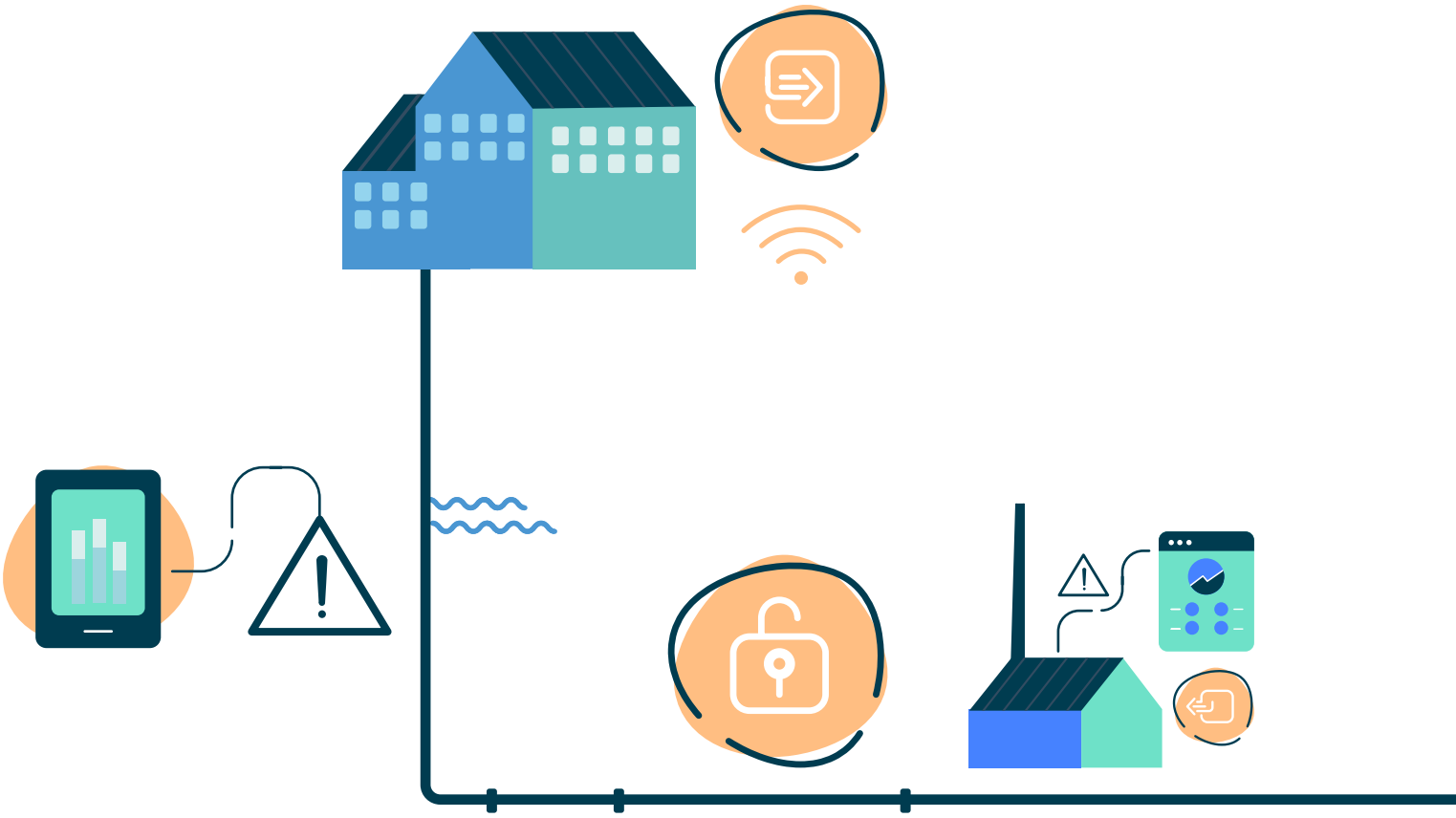
Sous couvert des dispositions de la transposition française, les obligations pour les entités régulées seront les suivantes :

- Définition et mise en œuvre d'une politique relative à l'analyse des risques et à la sécurité des systèmes informatiques ;
- Gestion des incidents ;
- Continuité des activités ;
- Sécurisation de la chaîne d'approvisionnement (fournisseurs, prestataires) ;
- Sécurisation de l'acquisition, du développement et de la maintenance des systèmes informatiques ;
- Définition et mise en œuvre des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
- Définition et mise en œuvre des pratiques de base ;
- Définition et mise en œuvre des procédures relatives à l'utilisation de la cryptographie ;
- Définition et mise en œuvre de la sécurité des ressources humaines, des politiques de contrôle d'accès et de gestion des actifs ;

- Définition et mise en œuvre de l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéographiques ou textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité selon les besoins.

Dans l'attente de la transposition en droit français, les entités essentielles se définissent par un personnel supérieur à 250 personnes et un chiffre d'affaires supérieur à 50 M € et les entités importantes par un personnel supérieur à 50 personnes et un chiffre d'affaires supérieur à 10 M €. Ces définitions s'appliquent bien aux entreprises, mais devront être adaptées lors de la transposition pour les collectivités et les administrations.

Par ailleurs, la directive sur l'eau potable publiée le 16 décembre 2020 rend obligatoire les plans de gestion de la sécurité sanitaire des eaux (PGSSE) à horizon 2027/2029. Le PGSSE intègre la prise en compte des risques en matière de cybersécurité.



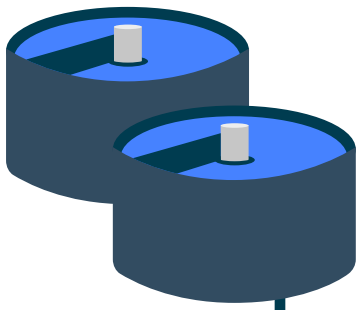
2. Le référentiel cybersécurité Astee

Le référentiel Astee présente les thèmes regroupant les différentes mesures de sécurité organisationnelles et techniques. Il s'inspire de l'expertise des membres du groupe de travail qui traite de la cybersécurité au sein de l'Astee ainsi que des guides de cybersécurité du domaine, et notamment ceux de l'ANSSI.

Ces mesures s'adressent à l'ensemble des acteurs impliqués dans la mise en œuvre et la gestion des systèmes industriels (responsables de collectivités, exploitants, automaticiens, intégrateurs, développeurs, équipes de maintenance, RSSI, etc.). Elles permettent de répondre aux exigences et objectifs de sécurité établis lors de l'analyse de risque préliminaire du système. Cependant elles ne peuvent se suffire à elles-mêmes et entrent dans une démarche globale de sécurisation, et n'ont pas vocation à remplacer celles des référentiels officiels (ANSSI, ISO, NIS2, etc.).

L'ensemble de ces mesures sont regroupées autour de 12 thèmes résumés ci-dessous. Pour chacun de ces thèmes, le référentiel Astee détaille les actions à mettre en place et les recommandations à suivre.

- Responsabilité des acteurs ;
- Connaissance du système d'informatique industrielle ;
- Sécurité de l'architecture informatique industrielle ;
- Sécurité des accès physiques ;
- Sécurité des accès logiques ;
- Maîtrise et configuration des équipements ;
- Maintenance et gestion des changements ;
- Détection et traitement des incidents ;
- Sauvegardes et continuité du service ;
- Audit, contrôle, suivi des indicateurs ;
- A. Éléments contractuels ;
- B. Sensibiliser et former le personnel.



0. Prérequis

Pour mettre en œuvre une politique de cybersécurité sur ses installations, il conviendra d'identifier les systèmes d'information et pour chacun d'eux, leur niveau de criticité et de sensibilité au regard du métier. Pour cela une analyse de risque constitue le prérequis indispensable à la poursuite d'une démarche de sécurisation.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Quel est le périmètre de vos services d'eau et d'assainissement à inclure prioritairement dans la démarche cybersécurité ?	**0-** Le périmètre n'est pas défini. **1-** Le périmètre n'est pas défini mais la démarche est en cours. **2-** Le périmètre inclut a minima un secteur des services industriels. **3-** Le périmètre intègre complètement un service industriel. **4-** Les services sont tous inclus dans le périmètre.	4	À définir pour tout ou partie des entités de gestion et des services (eau, assainissement, distribution, production, collecte, traitement...).	4	Idem petite structure.
1	Avez-vous mené une analyse afin d'évaluer la criticité et la sensibilité de vos équipements et systèmes d'informatique industrielle ?	**0-** L'analyse de risques n'a pas été réalisée. **1-** Une analyse informelle des risques liés aux principaux composants du système industriel a été réalisée. **2-** L'analyse de risque des principaux composants a été réalisée. **3-** L'analyse de risque de tous les composants a été réalisée. **4-** L'analyse de risque a été réalisée et est revue régulièrement.	2	Les dysfonctionnements de l'informatique industrielle sont à prendre en compte en réalisant une analyse des risques industriels et de leurs impacts sur la continuité de service et sur les aspects sanitaires, environnementaux, juridiques et économiques.	4	Idem petite structure.

1 du plus prioritaire, au 3 le moins prioritaire

1. Responsabilité des acteurs

Il est nécessaire de définir et nommer une chaîne de responsabilités de la cybersécurité permettant le fondement d'une bonne gouvernance. Cette chaîne vise à sensibiliser et responsabiliser les acteurs afin de :

- planifier, acquérir et mettre en œuvre les mesures de sécurité,
- maintenir les règles et mesures de sécurité,
- se tenir informé de la menace,
- diffuser les bonnes pratiques de cybersécurité.

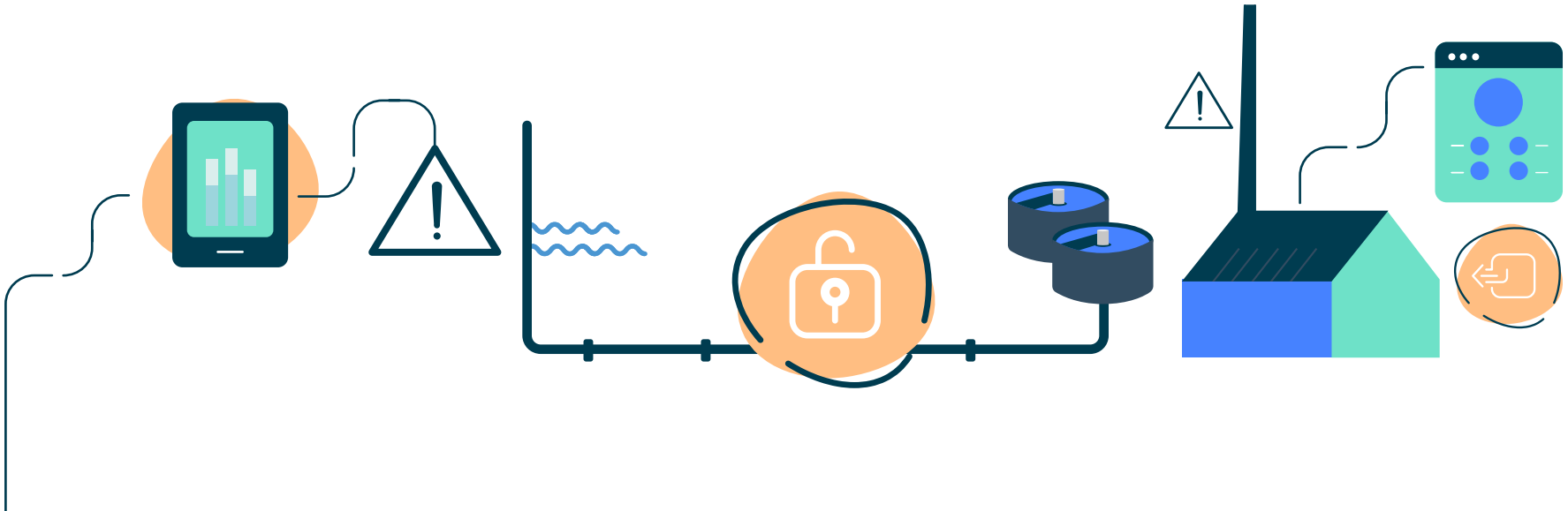
Elle doit être clairement discutée et identifiée avec l'ensemble des intervenants externes ou internes aux installations industrielles et notamment la collectivité, l'exploitant et les prestataires. En complément, la mise en place d'une politique de sécurité nécessitera des dépenses. Il faudra évaluer et allouer des budgets et potentiellement prévoir des investissements.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Avez-vous défini les responsabilités de chacun des acteurs internes ou externes (prestataires, délégataires…) concernés par la cybersécurité de vos installations industrielles ?	**0-** Aucune gouvernance n'est en place, les rôles et responsabilités ne sont pas définis. **1-** Une gouvernance informelle a été définie. **2-** Les rôles et responsabilités sont définis avec les principaux acteurs concernés par la cybersécurité, en particulier le référent technique, et leurs compétences sont validées. **3-** Les rôles et responsabilités sont définis avec l'ensemble des acteurs pouvant être concernés par la cybersécurité. **4-** La gouvernance est revue quand il y a des changements d'organisation.	2	• Organisation de la gouvernance (principe R.A.C.I.). • Identifier et nommer les acteurs clés de la cybersécurité, notamment un référent technique cybersécurité, et un Élu. La liste doit être maintenue à jour et diffusée.	4	• Formalisation des responsabilités au sein d'un document cybersécurité validée par les instances de direction. • Revue régulière (ex. annuelle) de ces responsabilités.
2	Avez-vous évalué et alloué (vous et votre éventuel délégataire) les budgets nécessaires pour améliorer le niveau de cybersécurité de vos installations industrielles ?	**0-** Pas de financement prévu. **1-** Estimation budgétaire indicative définie. **2-** Proposition précise de budget établie, éventuellement étalée dans le temps. **3-** Budget voté par la collectivité. **4-** Budget voté par la collectivité, et investissements à réaliser. Si DSP, les conditions de retour en fin de contrat sont définies.	4	• Après analyse des besoins en cybersécurité, il revient à la collectivité de financer les investissements physiques, logiciels et de digitalisation. • En cas d'exploitant privé, définir dans le contrat les investissements matériels et immatériels éventuellement inclus dans sa prestation et définir les conditions de retour en fin de contrat.	4	Idem petite structure.

2. Connaissance du système d'informatique industrielle

Les systèmes d'informatique industrielle ont la réputation d'être des systèmes d'information dont il est difficile de connaître les composants et l'environnement d'exploitation. Il est essentiel d'acquérir une connaissance précise et complète du système pour pouvoir lui appliquer les mesures de sécurité dont il fait l'objet. Ces éléments doivent être accessibles en cas de cyberattaque et d'indisponibilité des systèmes d'information, par exemple avec une version imprimée.

- **Cartographie :** il convient de disposer d'une connaissance complète de l'ensemble des constituants du système d'information à travers une cartographie. Cette cartographie doit être suivie et mise à jour régulièrement. Elle s'intègre dans une démarche générale de gestion des risques permettant de disposer d'une vision commune et partagée du système au sein de l'établissement afin de :
  - faciliter la prise de décision,
  - identifier les systèmes critiques et exposés,
  - réagir et prévoir efficacement les scénarios de défense en cas d'attaque,
  - identifier les fonctions nécessaires à la gestion de crise.
- **Inventaire des comptes informatiques :** il est nécessaire de disposer d'un inventaire des comptes informatiques qui peuvent se connecter au système d'information et leurs modalités d'accès.
- **Gestion des intervenants :** des procédures d'arrivée, de départ et de changement des agents qui interviennent sur les ouvrages devront être mis en place afin d'avoir une connaissance des intervenants et permettre notamment un contrôle des accès aux installations et aux équipements.
- **Gestion de la documentation :** en ce qui concerne la conception, l'exploitation et la maintenance des systèmes industriels, une documentation détaillée doit être rédigée et sauvegardée afin de maîtriser avec exactitude l'exploitation des processus. Cette documentation intègre notamment les analyses fonctionnelles, schémas d'architecture et plans d'adressage. Le plan doit prévoir une tenue à jour et une sauvegarde maîtrisée (lieu de stockage et journalisation des mises à jour) de ces documents.



			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Connaissez-vous suffisamment l'architecture de votre informatique industrielle ?	**0-** Cartographie inexistante. **1-** Disposez-vous d'une cartographie partielle des principaux systèmes ? **2-** Disposez-vous d'une cartographie de l'ensemble des sites et intersites (<2 ans). **3-** Le site dispose d'une cartographie complète et mise à jour régulièrement. **4-** Et à chaque modification d'architecture et de matériel.	2	• La cartographie doit comprendre un inventaire des logiciels, des connexions avec l'extérieur et leurs horaires, des flux et des traitements de données. • Cet inventaire doit être mis à jour à chaque modification (ajout/retrait sur le réseau IP d'équipement ou de logiciel, changement de paramétrage, de processus, etc.). • La cartographie doit être vérifiée régulièrement (<2 ans).	4	Idem petite structure.
2	Gérez-vous les procédures d'arrivée, de départ et de changement de fonction des agents de la collectivité ou de l'exploitant habilités à intervenir et/ou à gérer les installations ?	**0-** Pas de procédure de gestion des arrivées/départs. **1-** Procédure informelle de gestion des arrivées/départs et des changements de postes. **2-** Procédure formalisée des arrivées/départs et des changements de poste. **3-** La connaissance de la procédure est contrôlée régulièrement. **4-** Revue régulière de la procédure (<2 ans).	2	• Processus, à *minima* oral/informel. Revue régulière (<2 ans).	4	Processus formalisé avec contrôle continu. Revue régulière (ex. trimestrielle).
3	Comment gérez-vous la documentation technique et administrative relative aux systèmes d'information ?	**0-** Il n'existe pas de documentation et de logique de classification et de manipulation des documents, aucun mécanisme de contrôle d'accès n'est mis en place. **1-** La documentation existe. **2-** Et les accès aux documents sont restreints. **3-** Les documents sont classifiés avec définition des droits d'accès. **4-** Et sa mise en œuvre est contrôlée et l'utilisation des outils suit un processus.	2	• Disposer d'une version papier et d'une version électronique avec une sauvegarde hors site / hors ligne. • Garder un historique des mises à jour.	4	Idem petite structure, plus : • Classification des documents. • Contrôle d'accès. • Mise à jour en parallèle des versions électroniques et papier. • Revue régulière de la documentation.

3. Sécurité de l'architecture informatique industrielle

Le thème de la *Sécurisation de l'architecture du système industriel* aborde la structuration de l'architecture du système ainsi que la sécurisation des différentes interconnexions et échanges (communications, flux, protocoles) au sein du système lui-même et vers l'extérieur. Ce thème regroupe ainsi les catégories suivantes :

- **Cloisonnement des systèmes industriels :** il s'agit de penser les architectures en zones cloisonnées selon les fonctions ou nécessités techniques du système. Par ailleurs, il est nécessaire de prévoir les mécanismes de protection liés à ces cloisonnements (filtrage, segmentation physique ou logique le cas échéant…). Il est également fortement recommandé que le réseau d'administration soit cloisonné des autres réseaux. Selon la sensibilité de certains systèmes, il peut être demandé de maîtriser encore davantage le cloisonnement et les flux avec l'emploi d'équipements qualifiés ANSSI (emploi d'une diode ou d'un firewall labellisé par exemple).

- **Interconnexion avec le système d'information de gestion :** il s'agit de reprendre les éléments de la catégorie précédente en appliquant les mesures de protection (filtrage, gestion des flux…) au niveau de l'interconnexion avec le système d'information de gestion.

- **Accès Internet et interconnexions entre sites distants :** les interconnexions du système avec Internet (ou à d'autres systèmes via Internet) doivent être limitées et protégées via des mécanismes robustes voire qualifiés selon le niveau de sensibilité de l'installation.

- **Accès distants :** si la télémaintenance/télégestion est déployée, elle doit être maîtrisée (sonde de détection, journalisation…).

- **Systèmes industriels distribués :** concernant ces systèmes, ils se doivent d'utiliser des réseaux et protocoles protégés et maitrisés, en s'appuyant sur des solutions sécurisées dédiées (passerelle VPN, firewall, sonde de détection…) en privilégiant des liaisons louées avec des ressources dédiées aux réseaux publics.

- **Communications sans fil :** l'usage de technologies sans fil doit être limité au strict nécessaire tandis que les communications ainsi que les équipements doivent être cloisonnés au maximum, sécurisés et surveillés en fonction de la criticité du système.

- **Sécurité des protocoles :** lorsque c'est possible, les protocoles non sécurisés devraient être désactivés au profit des protocoles sécurisés. Sinon, des mesures de protection périmétriques doivent être mises en place (Pare-feu, VPN…).

- **Gestion de l'obsolescence :** les équipements et logiciels utilisés sur le système peuvent faire l'objet d'obsolescence laissant de nouvelles portes d'accès aux cyberattaquants. Il convient de prévoir en amont cet aspect en l'intégrant dans les contrats signés avec les fournisseurs et en établissant un plan de gestion d'obsolescence des composants.

L'ensemble de ces exigences de sécurité doivent être prises en compte lors de la conception initiale de l'architecture de l'informatique industrielle et lors des projets de travaux.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Intégrez-vous des exigences de sécurité lors de la conception initiale de l'architecture de l'informatique industrielle et lors des projets de travaux ?	**0-** Pas d'exigences particulières. **1-** Le site s'appuie sur le déclaratif et sur l'application de la politique de cybersécurité. **2-** Des exigences de cybersécurité sont intégrées dans le Cahier des Charges du projet. La cohérence de la proposition cyber et son coût sont évalués dans l'analyse des offres. **3-** Une analyse de risques et un Plan d'Assurance Sécurité (PAS) sont réalisés. Des mesures de sécurité spécifiques au projet selon les enjeux sont définies pendant la phase de spécification et vérifiées dans le PV de recette. **4-** Les risques résiduels sont évalués et acceptés. **N/A :** non applicable s'il n'y pas eu de travaux sur le SCI depuis 5 ans.	2	Exigences cybersécurité intégrées dans l'approche projet.	4	Rédaction des clauses cybersécurité du cahier des charges par un expert interne ou tiers.
1	Votre réseau d'informatique industrielle est-il isolé des réseaux tiers (réseau informatique de gestion, Internet) ?	**0-** Les deux réseaux ne sont pas cloisonnés. **1-** Les deux réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont interconnectés sans filtrage. **2-** Les deux réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont isolés par des pare-feux avec filtrage. **3-** Et la matrice de flux n'autorise que les flux strictement nécessaires. Un processus de gestion des changements des flux est en place. **4-** Et le cloisonnement est documenté et revu de façon régulière, ou les réseaux ne sont pas interconnectés et sont physiquement isolés. **N/A :** s'il n'y a pas de réseaux tiers sur le site industriel.	2	Réseaux industriels et informatique de gestion physiquement isolés.	4	• Réseaux industriels et informatique de gestion physiquement isolés. **OU** • Cloisonnement avec pare-feu. Le pare-feu doit être à jour et toute modification doit être contrôlée.
2	Si vous avez plusieurs réseaux d'informatique industrielle, sont-ils isolés entre eux ?	**0-** Les réseaux ne sont pas cloisonnés. **1-** Les réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont interconnectés sans filtrage. **2-** Les réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont isolés par des pare-feux avec filtrage. **3-** Et la matrice de flux n'autorise que les flux strictement nécessaires. Un processus de gestion des changements des flux est en place. **4-** Et le cloisonnement est documenté et revu de façon régulière, ou les réseaux ne sont pas interconnectés et sont physiquement isolés. **N/A :** s'il n'y a qu'un seul réseau industriel.	3	Pas d'interconnexion entre les différents réseaux d'informatique industrielle.	4	• Pas d'interconnexion entre les différents réseaux d'informatique industrielle. **OU** • Cloisonnement entre les différents réseaux d'informatique industrielle (réseau virtuel local + Pare Feu ou VPN). Le cloisonnement doit être contrôlé régulièrement et un processus de gestion des changements est mis en place.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Si vous gérez les contrôles d'accès dans vos locaux industriels, le réseau qui les gère est-il distinct de votre réseau d'informatique industriel ?	**0-** Les réseaux ne sont pas cloisonnés. **1-** Les réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont interconnectés sans filtrage. **2-** Les réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont isolés par des pare-feux avec filtrage. **3-** Et la matrice de flux n'autorise que les flux strictement nécessaires. Un processus de gestion des changements des flux est en place. **4-** Et le cloisonnement est documenté et revu de façon régulière, ou les réseaux ne sont pas interconnectés et sont physiquement isolés. **N/A :** s'il n'y a pas de réseau de sûreté physique.	2	• Cloisonnement avec pare feu. OU • Réseaux physiquement isolés.	4	Idem petite structure.
2	Si vous avez un exploitant, comment sont gérés les échanges entre votre réseau informatique et celui de l'exploitant ?	**0-** Les réseaux collectivité et exploitant ne sont pas cloisonnés. **1-** Les réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont interconnectés sans filtrage. **2-** Les réseaux sont segmentés en deux réseaux logiques (VLAN) ou physiques, et sont isolés par des pare-feux avec filtrage. **3-** Et la matrice de flux n'autorise que les flux strictement nécessaires. Un processus de gestion des changements des flux est en place. **4-** Et le cloisonnement est documenté et revu de façon régulière, ou les réseaux ne sont pas interconnectés et sont physiquement isolés. **N/A :** s'il n'y a pas de liaison vers le réseau de la collectivité.	2	L'accès en continu aux données par la collectivité est fourni par l'exploitant de manière sécurisée et authentifiée.	4	Idem petite structure.
1	Comment sont gérés les accès internet vers/depuis votre réseau d'informatique industrielle de contrôle-commande ?	**0-** Internet est accessible sans restriction et les réseaux industriels est visible d'internet. **1-** Les opérateurs sont sensibilisés aux bonnes pratiques d'utilisation d'internet et les réseaux industriels ne sont pas visibles depuis Internet. **2-** Et les navigateurs liés aux équipements ont été durcies (plug in, etc). **3-** Et le trafic n'est autorisé que pour l'accès à certains sites ou catégories de sites et les règles sont revues régulièrement. **4-** Internet n'est pas accessible directement depuis / vers les réseaux industriels. **N/A :** il n'y a aucune connexion depuis/vers Internet.	2	Les accès des réseaux industriels depuis/vers Internet sont sécurisés.	4	Idem petite structure.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Comment sont sécurisées les éventuelles connexions sans fil entre les équipements (WiFi, 2-5G, Bluetooth, GSM) ?	**0-** Aucun mécanisme de sécurité n'est mis en œuvre. **1-** Les réseaux sans fil sont limités au strict nécessaire. Les autres points d'accès sont désactivés. **2-** Les accès sans fil sont protégés par un mécanisme d'authentification. **3-** Et revus régulièrement (<2 ans). **4-** Les points d'accès sont journalisés (authentifications et tentatives, alertes automatiques). **N/A :** s'il n'y a pas de réseau sans fil.	2	• Utilisation du réseau Wifi industriel, 4G/5G et radio envisageables si sécurisée (chiffrement+authentification). • Remplacement des équipements 2G/3G avant arrêt par les opérateurs télécoms.	4	Suivi des accès et contrôle des accès.
1	Comment sont sécurisés les accès à distance pour la gestion et la maintenance de vos équipements industriels ?	**0-** Les accès distants ne sont pas identifiés ou non sécurisés. **1-** Les accès distants utilisent une passerelle VPN, avec durée de session limitée. **2-** Et sont authentifiés. **3-** Au moyen d'une authentification forte nominative. **4-** Et un serveur de rebond dans une DMZ est utilisé. **N/A :** il n'y a aucun accès distant.	2	• Accès distant seulement via VPN avec authentification simple. Les accès sont contrôlés avec coupure automatique des connexions après un temps d'inactivité.	4	Authentification forte et serveur de rebond.
3	Avez-vous une politique de gestion des risques vis-à-vis de vos équipements mal sécurisés (anciens automates, modem, OS, ...) ?	**0-** Les équipements non ou mal sécurisés (vieux automates, modems, vieux OS non maintenus, etc.) ne sont pas identifiés. **1-** Les équipements non ou mal sécurisés sont identifiés. **2-** Et un plan de remédiation a été défini (durcissement, protection périmétrique, remplacement, acceptation de risque résiduel, etc.). **3-** Le plan de remédiation a été réalisé et les équipements sont sécurisés. **4-** Et les équipements sécurisés font l'objet d'un suivi régulier.	2	• Les équipements vétustes (obsolètes, maintenance n'étant plus assurée) doivent être identifiés et remplacés. Ex : automates, serveurs, systèmes d'exploitation et outils logiciels d'ancienne génération. • Les équipements ne pouvant être remplacés font l'objet d'une protection spécifique. Ex : filtrage des flux, filtrage des accès.	4	Une revue technique régulière des équipements est organisée (ex : annuelle). • Suivi de la fin de vie des équipements. • Remontée des revues aux instances décisionnelles. • Privilégier les équipements qualifiés ou certifiés par l'ANSSI.

4. Sécurité des accès physiques

- **Accès aux locaux et aux équipements :** une politique de gestion des accès aux locaux doit être mise en œuvre pour permettre un accès approprié aux intervenants. Une vigilance particulière sera adressée aux prestataires et intervenants externes. L'installation d'un système de contrôle des accès sera nécessaire et permettra de mettre en œuvre cette politique de gestion des accès.

- L'ensemble des composants du système seront sous contrôle d'accès et placés dans des locaux ou des armoires fermées à clé. *A minima*, les prises et moyens de connexions au système ne devront pas être accessibles au public. Pour les systèmes les plus critiques, câbles et prises feront l'objet d'une sécurisation complémentaire.

- **Protection vis-à-vis des dommages physiques :** la sécurité des installations dépend de leur protection vis-à-vis des risques tels que les incendies ou les inondations. Les moyens de détection et de protection de ces phénomènes devront être pris en considération.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Avez-vous sécurisé l'accès physique à vos locaux abritant des équipements industriels ?	**0-** Les locaux sont accessibles sans contrôle d'accès. **1-** Les locaux sont accessibles avec un contrôle d'accès (badge, clef, digicode…) mais non restreints aux seuls utilisateurs ayant le besoin d'accéder aux locaux. **2-** Les accès aux locaux sont restreints aux seules personnes autorisées et les demandes d'accès sont inventoriées. **3-** Et une procédure formalisée existe pour les demandes d'accès. Une revue des accès est réalisée régulièrement. **4-** Tous les accès sont tracés et sauvegardés durant une durée déterminée et les anomalies sont gérées proactivement.	2	• Contrôle régulier de l'état des ouvrants. • Mise en place d'un contrôle d'accès sur chaque site avec accès restreint nominatif et enregistrement des demandes d'accès.	4	Procédures formalisées d'attribution et de suivi des accès.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	L'accès aux systèmes de commande de vos équipements industriels est-il restreint et contrôlé ?	**0-** Les équipements sont accessibles sans contrôle d'accès. **1-** Les équipements sont accessibles avec un contrôle d'accès (mais non restreints aux seuls utilisateurs ayant le besoin d'accéder aux équipements). **2-** Et restreint aux seuls utilisateurs ayant le besoin d'accéder aux équipements. **3-** Et les connectivités (USB, Port RJ45,...) non utilisées sont désactivées ou bloquées. **4-** Et les demandes d'accès sont inventoriées, contrôlées et revues régulièrement.	2	Accès limité aux équipements sensibles.	4	• Les connectivités non utilisées sont identifiées et sécurisées. • Procédure formalisée d'accès.
2	Vos équipements de contrôle-commande sont-ils protégés vis-à-vis des risques de dommages physiques (feu, eau, coupures de courant, ...) ?	**0-** Aucune protection particulière n'est prévue. **1-** Les principaux équipements sont hébergés dans des endroits dédiés (salle, baie, armoire, etc.). **2-** Et disposent des protections usuelles (ventilation, climatisation, détection d'incendie, onduleur, filtre à particules, etc.). **3-** Et ces protections sont opérationnelles, maintenues régulièrement et disposent d'une protection incendie adaptée et complétée par une protection incendie pour les principaux sites. **4-** Une analyse de risque des conditions d'usage a été réalisée.	2	• Protéger les équipements des risques de dégâts physiques. • Détection d'incendie, température élevée, humidité, inondation, ...	4	• Mener une analyse de risque. • Mise en place de protection incendie adaptée.

5. Sécurité des accès logiques

Ce thème couvre les aspects liés à la gestion de l'identification et l'authentification des utilisateurs du système. Ces catégories sont :

- **La gestion des comptes :** elle regroupe les différentes règles permettant d'identifier chaque utilisateur, compte et rôle associé afin de les maîtriser et limiter les privilèges associés à chacun d'eux en se donnant la possibilité de les contrôler. Une attention particulière est portée sur les comptes à forts privilèges tels que les comptes d'administration.
- **La gestion de l'authentification :** elle aborde les mécanismes inhérents à l'accès aux différents composants constituants le système (physique et logique) ainsi que la protection des secrets associés à ces mécanismes en appliquant une politique de sécurité liée aux mots de passe. Une attention particulière sera appliquée sur la complexité des mots de passe et leur renouvellement.
- **La gestion de l'inventaire :** elle permet la création et le maintien à jour d'un inventaire des comptes logiques et des habilitations déterminées en fonction des rôles.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
3	Limitez-vous au maximum l'utilisation de comptes génériques ?	**0-** Les comptes (utilisateurs, administrateurs, autres) ne sont pas authentifiés nominativement, les comptes génériques ne sont pas listés. **1-** Les comptes génériques et de service sont listés et justifiés. **2-** La liste des personnes ayant la connaissance du mot de passe du ou des comptes génériques est maintenue à jour. **3-** Et les actions tracées pour tout accès et toute modification. **4-** Tous les utilisateurs sont authentifiés nominativement et les actions tracées et les mots de passe des comptes génériques sont changés lorsqu'un utilisateur en ayant la connaissance n'a plus lieu de l'utiliser.	2	• Les comptes d'accès nominatifs doivent être privilégiés. • L'existence de comptes génériques doit être justifiée. Ils doivent être inventoriés. • Un système de traçabilité permet de savoir qui a effectué des modifications. Ces traces sont sauvegardées et accessibles en cas de besoin.	4	• Les comptes d'accès sont nominatifs. • Visibilité sur les actions des utilisateurs.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Les personnes habilitées à accéder informatiquement sur vos équipements industriels sont-elles identifiées et leurs interventions sont-elles autorisées ?	**0-** Il n'existe pas de comptes utilisateurs : les utilisateurs ne sont ni identifiés ni authentifiés et aucune mesure alternative n'est implémentée. **1-** Les utilisateurs sont identifiés par un identifiant, sans authentification. **2-** Identifiés, et authentifiés. **3-** Authentification forte selon le risque/criticité. **4-** Processus formalisé de suivi des authentifications.	2	Identifier et authentifier les accès.	4	• Authentification renforcée selon le risque/la criticité de la tâche. • Processus de suivi.
3	Avez-vous inventorié les comptes informatiques qui peuvent se connecter au système d'information et leurs modalités d'accès (connexion locale ou distante) ?	**0-** Pas d'inventaire. **1-** Inventaire informel. **2-** Inventaire formel des principaux comptes. **3 -**Inventaire formel de tous les comptes. **4-** Inventaire revu régulièrement suivant un processus formalisé.	2	Inventorier les comptes à privilège (ex. compte administrateur, compte avec droits de modification…) qui peuvent se connecter au système d'information et leurs modalités d'accès (connexion locale ou distante).	4	• Inventorier l'ensemble des comptes qui peuvent se connecter au système d'information et les modalités d'accès (connexion locale ou distante). • Formaliser un processus régulier de revue de ces comptes, *a minima* annuel.
3	Disposez-vous d'un inventaire des comptes informatiques de vos utilisateurs ?	**0-** Aucune disposition particulière n'est prise pour les demandes et la revue des comptes. **1-** Les utilisateurs des comptes logiques sont inventoriés. **2-** Et l'inventaire est revu régulièrement en fonction du mouvement du personnel (arrivée, départ, extension de droits, changement de poste/responsabilité). **3-** Et leur application est contrôlée, documentée et suis un processus formalisé. **4-** Et audité régulièrement (<2 ans).	2	Mettre à jour régulièrement l'inventaire des comptes logiques, en particulier lors des prises de poste.	4	Disposer de moyen de contrôle et d'alerte en cas de modifications.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
3	Avez-vous défini les habilitations de chaque compte utilisateur par rapport à son besoin d'accès ?	**0-** Aucune gestion des habilitations. **1-** Une gestion des habilitations est effectuée de manière informelle. **2-** Une gestion des habilitations est définie et appliquée. **3-** Et fait l'objet d'un suivi attentif, régulier, formalisé dans une matrice/tableau. **4-** Et revu, audité et réajusté si nécessaire (1x /an).	2	• Définir les habilitations de chaque compte utilisateur par rapport à son besoin d'accès. • Revoir régulièrement les habilitations (*a minima* tous les ans) afin de respecter le principe de moindre privilège.	4	• Documentation d'une matrice/ tableau des droits. • Document de suivi des revues et audits avec historisation des modifications et diffusion à la hiérarchie du travail réalisé.
2	Quelle est votre politique d'utilisation de mots de passe ?	**0-** Les utilisateurs ne sont pas authentifiés. **1-** Les utilisateurs utilisent un mot de passe sans contraintes, mais différent du mot de passe par défaut. **2-** Les utilisateurs utilisent un mot de passe avec contraintes, issu d'une politique de mot de passe (nombre de caractères, niveau de complexité, durée de validité…)? **3-** Et est appliquée de manière uniforme la politique de sécurité. Les comptes d'administration font l'objet d'une politique endurcie. **4-** Et les utilisateurs emploient un mécanisme d'authentification forte (ex : carte à puce + PIN) pour les actes d'administration.	2	• Les mots de passe sont complexes et renouvelés régulièrement. • Les mots de passe constructeur doivent systématiquement être modifiés lors de la mise en service des équipements.	4	Les mots de passe sont déterminés suivant une politique définie de mot de passe.
3	Comment sont gérés et sauvegardés vos mots de passe ?	**0-** Les mots de passe sont disponibles et visibles dans des fichiers texte numérique ou papier. **1-** Les mots de passe sont stockés dans un coffre-fort électronique. **2-** Et sauvegardé hors-ligne. **3-** Les mots de passe sont gérés selon des profils d'utilisateur. **4-** L'accès au coffre-fort est surveillé et tracé.	2	Les mots de passe doivent être stockés dans un gestionnaire de mot de passe. Ex : Keepass, Lockself, Bitwarden, Vaultwarden, …	4	Une procédure d'alerte, verrouillage et changement de mots de passe existe en cas de perte, vol ou compromission.

6. Maîtrise et configuration des équipements

Le thème sur la Sécurisation des équipements présente les aspects liés à la sécurisation des équipements utilisés au sein du système ainsi que la sécurisation de leur configuration et leur maintien dans le temps :

- **Habilitation et formation :** les personnes intervenant sur les ouvrages doivent être formées et habilitées à intervenir. Une charte d'utilisation permet de formaliser ces aspects.
- **Durcissement des configurations :** il s'agit de désactiver tout ce qui n'est pas nécessaire au fonctionnement du système mais aussi de mettre en place les mécanismes permettant une sécurisation supplémentaire des accès au programme tel que la mise en place de liste blanche des applications autorisées à s'exécuter.
- **Protection des postes et serveurs :** il s'agit de désactiver tout ce qui n'est pas nécessaire au fonctionnement du système mais aussi de mettre en place les mécanismes permettant une sécurisation supplémentaire tels que des antivirus et EDR.
- **Gestion de l'obsolescence :** les composants d'un système industriel sont destinés à être exploités durant de nombreuses années. Afin de conserver leur maîtrise dans le temps et notamment leur obsolescence, il conviendra d'inventorier les dates de fin de maintenance et d'assistance technique. Une anticipation sur leur renouvellement ou leur modernisation devra être organisée.
- **Équipements mobiles :** sur le même principe, dans le cas de l'utilisation d'équipements mobiles, leur emploi doit être maîtrisé, limité et dédié au système industriel.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Les personnes habilitées à intervenir sur vos équipements industriels sont-elles identifiées et formées ?	**0-** Aucune mesure n'est mise en œuvre. **1-** Une notification orale de l'utilisation correcte des équipements est effectuée avant l'accès aux équipements industriels. **2-** Une charte d'utilisation des équipements industriel est formalisée, validée par la structure, et signée par le personnel concerné. **3-** Et la charte est régulièrement mise à jour et diffusée au personnel. **4-** Et seul le personnel habilité peut utiliser l'équipement.	2	• L'accès doit être limité aux personnes formées et habilitées à intervenir sur l'équipement. • La liste de ce personnel doit être considérée comme sensible et sécurisée. • S'assurer de la bonne connaissance de la charte utilisateur.	4	Définir et mettre en place un système de contrôle des équipements informatiques industrielles, par un contrôle d'accès physique et logique aux équipements.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	La configuration des équipements d'informatique industrielle et des postes de travail et terminaux nomades ayant accès aux systèmes industriels est-elle sécurisée ?	**0-** Aucune mesure de durcissement n'est appliquée. **1-** Un ensemble de mesures permettant de durcir le système est défini. **2-** Appliqué et contrôlé. **3-** Des mesures spécifiques sont appliquées aux équipements au cas par cas. **4-** Sont documentés et suivent un processus d'audit et conformité.	2	• Configurer les équipements et les outils logiciels en respectant strictement les préconisations de sécurisation. • Ex : désactivation de fonctionnalités non utilisées, sécurisation du bios, désactivation de ports, chiffrement des disques durs, ...	4	• Mettre en place un système centralisé de contrôle et suivi de la conformité. • Gérer une liste blanche d'applications permises dans le cadre professionnel sur les postes de travail reliés aux systèmes industriels. • Sécuriser/durcir les fonctionnalités utilisées.
3	Les équipements non maîtrisés par l'exploitant provenant d'intervenants externes (Ex : clés USB, ordinateur portable des agents de maintenance) sont-ils suffisamment sécurisés ?	**0-** Aucune mesure particulière n'est mise en œuvre. **1-** Les utilisateurs et prestataires sont informés qu'ils ne doivent pas connecter leurs équipements (clés USB, disque dur, téléphones, tablettes, PC portables...) sans suivre un processus défini. **2-** Seul les équipements dédiés au système industriel et sécurisés par le prestataire (antivirus, absence de boite email, etc.) doivent être utilisés sur site. L'antivirus local est configuré pour scanner automatiquement les équipements tiers. **3-** Et un contrôle des périphériques est réalisé notamment pour les PC portables et des mesures de sécurisation complémentaires ont été mises en place (lecture seule, blocage ou désactivation des ports USB, ...). **4-** Aucun équipement externe n'est utilisé sur site, seuls ceux fournis par l'exploitant peuvent se connecter.	2	Tout équipement amovible doit être fourni par l'exploitant ou contrôlé par un antivirus.	4	Autoriser et filtrer uniquement les périphériques fournis par l'entreprise.
2	Les médias amovibles utilisés par des intervenants internes (clés USB et autres disques portables) sont-ils contrôlés ?	**0-** Les médias amovibles ne sont pas maîtrisés. **1-** Les médias amovibles utilisés en interne ont été fournis en interne. **2-** Et ils sont référencés dans un inventaire. **3-** Et attribués nominativement à une personne ou un service (maintenance). **4-** Et ils sont dédiés à une seule fonction dans un seul environnement (sauvegarde, etc.). **N/A :** il n'y a aucun média amovible utilisé.	2	Médias sont fournis par l'exploitant, inventoriés, et dédiés aux systèmes industriels.	4	Les médias amovibles sont attribués nominativement et dédiés à une seule fonction (ex : récupération de données process, administration/ configuration du système, sauvegardes applicatives).

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Les postes de travail et serveurs sont-ils protégés contre les logiciels malveillants ?	**0-** Il n'existe pas de protection particulière. **1-** Des d'outils de détection basés sur des mécanismes de détection statique (ex: antivirus avec signature) sont utilisés. **2-** Et leur mise à jour est effectuée de façon régulière (au minimum annuellement). **3-** Et des outils de détection dynamique sont également utilisés (type EDR). **4-** Et les alertes remontées sont centralisées, analysées et traitées.	2	Logiciels antivirus et/ou EDR avec mise à jour automatique.	4	Les alertes sont tracées, centralisées et traitées par du personnel compétent avec un outil de gestion d'alertes dédié, ex : un SIEM.
3	Gérez-vous le risque d'obsolescence de vos matériels et logiciels en prenant en compte les risques cyber induits ?	**0-** Les systèmes en situation d'obsolescence ne sont pas identifiés. **1-** La date de fin d'assistance technique est connue. **2-** Et référencée dans l'inventaire. **3-** Et la date de remplacement est programmée. **4-** Un processus de migration de chaque système en situation d'obsolescence est documenté et suivi.	2	Tenir un inventaire à jour, avec dates de fin de support et de maintenance.	4	• Planifier à l'avance le renouvellement des systèmes. • Les processus de migration et de mise au rebut sécurisés sont documentés et suivis.
3	Gérez-vous de manière sécurisée la fin de vie des équipements ?	**0-** Pas de procédure de décommissionnement d'équipements. **1-** Les anciens équipements sont déconnectés du réseau. **2-** Les données des anciens équipements sont supprimées de manière sécurisée. **3-** La documentation technique est revue suite au décommissionnement. **4-** Les anciens équipements sont supprimés des listes d'accès réseau et des configurations des outils de sécurité.	2	• Déconnecter les équipements du réseau. • Supprimer les données avec un outil de suppression, ou bien détruire le stockage / disque dur.	4	• Vérifier la documentation réseau, comptes utilisateurs, systèmes. • Veiller à revoir les configurations des équipements réseau et de sécurité.

7. Maintenance et gestion des changements

- **Gestion des nouveaux équipements :** lors de la mise en exploitation de nouveaux équipements sur le système d'information, les mesures de protections cyber seront mis en œuvre. Des tests éventuels pourront être organisés.
- **Gestion des modifications et évolutions :** pour toute modification d'applications, les fichiers de configuration de l'ensemble des composants du système doivent être tracés. Une procédure est mise en place et son application contrôlée.
- **Gestion des interventions :** les interventions sur les systèmes industriels doivent faire l'objet d'une procédure organisée et tracée, décrivant l'ensemble des aspects essentiels à l'intervention. Il conviendra notamment de notifier et valider avec le responsable du système : l'identité de l'intervenant, la période et le périmètre d'intervention. L'ensemble des actions effectuées doit être décrit ainsi que les équipements permettant ces actions.
- **Gestion des intervenants :** les intervenants sur les systèmes industriels ont des profils différents (mainteneur, responsable technique, responsable d'exploitation…). Ils peuvent être internes ou être des prestataires extérieurs (fournisseurs, intégrateurs…). Il est essentiel de pouvoir gérer ces intervenants en fonction de leurs droits, fonctions, scope d'intervention. Cette gestion implique notamment une maîtrise à jour des accès aux locaux, au réseau, aux données ainsi qu'à l'utilisation d'équipements électroniques. Ces données d'accès doivent être conformes aux bonnes pratiques de gestion des identifiants.
- **Gestion des procédures d'urgence :** en cas d'intervention d'urgence sur les équipements, une procédure doit être appliquée et documentée.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Lors de la mise en place de nouveaux équipements, mettez-vous en place des mesures spécifiques de protection cyber ?	**0-** Aucune mesure de cybersécurité n'est mise en place avant la mise en exploitation d'un actif. **1-** Des règles informelles de durcissement des actifs sont connues. **2-** Et des mesures simples sont implémentées avant de mettre l'actif en exploitation (changement des mots de passe par défaut, …). **3-** Et des mesures spécifiques / complexes sont formalisées et implémentées avant de mettre l'actif en exploitation (durcissement de configuration, limitation des flux,…). **4-** Et des tests de sécurité sont effectués avant la mise en exploitation.	2	• Le durcissement physique et logiciel des équipements fait partie de l'approche projet. • Privilégier les équipements certifiés ou qualifiés par l'ANSSI.	4	La cybersécurité est vérifiée selon les exigences de sécurité applicables à l'équipement avant sa mise en service.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
3	Lors de modifications physiques ou logiques sur vos matériels, le risque cyber est-il intégré à la démarche ?	**0-** Aucun processus n'est mis en place. **1-** Un processus informel est suivi. **2-** Une procédure de gestion des modifications est documentée et appliquée. **3-** Et son application est contrôlée. Tout changement donne lieu à un compte-rendu. **4-** Et le risque lié à une modification est analysé et validé par un comité de validation des modifications et changements.	2	Mise en place de procédures de gestion des modifications.	4	Analyse du risque réalisée préalablement à l'intervention.
3	Avez-vous mis en place des procédures (fiches d'intervention, rapport, ...) permettant d'encadrer les interventions ?	**0-** Les interventions s'effectuent sans fiche d'intervention et/ou sans contrat avec les intervenants externes. **1-** Les interventions s'effectuent avec une fiche d'intervention (ordonnancement, ...) et dans le cadre d'un contrat. **2-** Dont le périmètre est défini. Un rapport d'intervention est rédigé pour chaque intervention. **3-** Un personnel interne accompagne les prestataires externes, ou réalise l'intervention. **4-** Les outils utilisés ont été contrôlés au préalable. Pour les intervenants externes, une clause de confidentialité a été signée.	2	Une fiche d'intervention est réalisée et validée pour cadrer chaque intervention.	4	Les interventions sont cadrées et suivies.
2	En cas d'intervention d'urgence sur les équipements d'informatique industrielle, avez-vous formalisé une procédure permettant de l'encadrer ?	**0-** Aucun processus n'est mis en place. **1-** Un processus informel est mis en place. **2-** Une procédure d'intervention d'urgence est documentée et appliquée, et est accessible facilement. **3-** Et testée, et connue par le personnel impliqué. **4-** Et la procédure d'intervention d'urgence est revue régulièrement et le bon fonctionnement des outils et accès sont vérifiés.	2	Processus formel qui précisera les intervenants et les formalités nécessaires.	4	• Cette procédure détaillera qui peut intervenir et les formalités nécessaires avant et après chaque intervention. • La procédure est testée et revue chaque année.

8. Détection et traitement des incidents

- **Processus de veille :** une veille liée au risque cyber doit être organisée et suivie dans le temps. À cet effet, les CERT ainsi que ceux des fabricants et éditeurs de logiciels doivent être consultés pour permettre une application des mesures adaptées aux tendances et failles identifiées.

La Surveillance du système industriel couvre la notion de traçabilité des évènements sur le système industriel, au travers de la catégorie suivante :

- **Journaux d'événements :** afin d'assurer la traçabilité des évènements sur le système, une politique de gestion doit être définie et mise en place comprenant : les évènements pertinents à tracer, leur conservation (stockage, archivage), les conditions d'analyse, ainsi que les alertes à générer.
- **Analyse des événements :** en cas d'incident, les événements journalisés peuvent être analysés afin de comprendre les causes et d'y remédier.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Avez-vous mis en place une veille et de gestion des risques cyber concernant vos équipements et logiciels ?	**0-** Aucun processus de veille en vulnérabilité n'existe. **1-** Un processus de veille et gestion des vulnérabilités est documenté et appliqué pour les systèmes d'exploitation et de sécurité informatique. **2-** Et son application est contrôlée. **3-** Le processus de veille en vulnérabilité s'appuie sur plusieurs sources différentes afin de s'assurer de l'exhaustivité des alertes. Les équipements industriels sont pris en compte. **4-** Si l'application d'un correctif n'est pas possible, des mesures palliatives sont implémentées.	2	• Veille sur les vulnérabilités, à minima des systèmes d'exploitation et des équipements de sécurité informatiques. Ex : via CERT-FR, CSIRT régional. • Effectuer les mises à jour de sécurité en cohérence avec l'analyse des risques. • Un outil de suivi des patchs est recommandé.	4	• Veille portant sur les vulnérabilités concernant tous les équipements de l'inventaire, dont notamment les équipements industriels. • Une analyse de risque est réalisée avant une intervention sur des équipements industriels et les mises à jour ou les modifications nécessaires sont réalisées en fonction d'une évaluation de leur criticité et de l'impact sur les systèmes. • Si un correctif est impossible ou indisponible, des mesures palliatives sont mises en place.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
3	Avez-vous mis en place une procédure permettant de suivre les actions réalisées sur le système de supervision et de sécurité informatique ?	**0-** Aucune journalisation des événements n'est effectuée ou avec une configuration par défaut. **1-** Les événements sont tracés et conservés localement. **2-** Les événements sont centralisés. **3-** Et des mécanismes simples sont en place pour augmenter le niveau d'intégrité des journaux (ex : synchronisation des horloges, sauvegarde hors ligne régulière, etc.). **4-** Et des mécanismes avancés sont en place pour augmenter le niveau d'intégrité des traces (ex : signature des journaux, accès contrôlé).	1	La conservation de l'historique des actions est activée si l'équipement le permet.	4	• Les événements sont centralisés. • Les communications inter équipements industriels sont tracées via des sondes IDS OT dédiés. • Les événements sont conservés pendant au moins 3 mois. • La confidentialité, l'intégrité et la disponibilité de la journalisation est garantie. Ex : par la signature des journaux, accès contrôlé.
3	Analysez-vous les événements en cas d'incident afin d'en comprendre les causes et y remédier ?	**0-** Les traces n'existent pas ou ne sont pas examinées. **1 -**Les traces sont examinées en cas de dysfonctionnement. **2-** Les traces sont examinées manuellement de façon régulière. **3-** Les traces sont examinées et corrélées, et des anomalies sont détectées par rapport à un processus de priorisation, à l'aide d'un outil de détection et de gestion de logs. **4-** Et un SOC, comprenant du personnel qualifié, veille en temps réel sur les alertes de sécurité.	1	Les événements sont analysés en cas d'incident afin d'en comprendre les causes et y remédier.	4	• Les événements sont analysés de manière automatique avec alertes. • Les alertes sont traitées proactivement par du personnel qualifié.
3	Une procédure formelle est-elle en place pour la gestion d'un incident d'origine cyber avéré ?	**0-** Aucune organisation liée à la gestion des incidents n'est en place. **1-** Une organisation informelle est en place. **2-** La procédure de gestion des incidents est documentée et connue. **3-** Et testée régulièrement, et les rôles et responsabilités ont été attribués. **4-** Et le processus est revu et amélioré après chaque incident.	2	Une procédure formelle est alors mise en place pour la gestion d'un incident avéré. Cette procédure inclura : Les modes de communication des acteurs internes. • Les acteurs externes cyber à solliciter en cas de crise et leurs coordonnées (référents territoriaux de l'ANSSI, CERT-FR, experts en cybersécurité…). • Les mesures d'urgence d'arrêt d'équipements. • La constitution d'une cellule de crise. • Les procédures de notification aux autorités et les délais (préfecture, procureur, CNIL, ANSSI, etc.). • La procédure de correspondance avec les médias. Cette procédure est disponible hors ligne et sur support papier.	4	La procédure est testée et revue/améliorée.

9. Sauvegardes et continuité du service

- **Plan de reprise ou de continuité d'activité :** un plan de reprise d'activité (PRA) et de continuité d'activité (PCA) doit être mis en œuvre. Le PRA doit permettre de prévoir par anticipation, les mécanismes pour reconstruire et relancer le système en cas de sinistre. Le PCA doit permettre de prévoir une stratégie qui limite l'impact d'un incident, quitte à ce que le service soit dégradé. Dans le cas où un PRA et un PCA existent déjà pour le fonctionnement du système, il faudra y intégrer les incidents de cybersécurité.

- **Gestion des sauvegardes :** un plan de sauvegarde doit être mis en place afin de disposer des données participant au bon déroulement d'un Plan de Reprise d'Activité (PRA) qui intervient après une attaque. Ce plan doit prendre en compte un suivi des sauvegardes à chaque modification. Les données à sauvegarder concernent les équipements serveurs, postes informatiques, automates et équipements terrain (capteurs, actionneurs), équipements réseau, équipement de sécurité. Pour l'ensemble de ces composants, les données à sauvegarder (lorsqu'elles existent) sont :
  - fichier d'installation logiciel,
  - base de données de configuration,
  - historian,
  - firmwares,
  - programmes automates,
  - fichier de configuration.

- **Test de restaurations des sauvegardes :** afin de s'assurer de la bonne restauration des données sauvegardées, une procédure sera rédigée et réalisée à des fins de test.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Avez-vous réfléchi à un plan de continuité des activités (PCA) en cas d'incident majeur ?	**0-** Aucun plan de continuité n'a été prévu. **1-** Le site a réalisé une analyse d'impact en cas de sinistre. **2-** Et le site a identifié ses processus critiques et les équipements contribuants à la continuité d'activité. **3-** Et un plan de continuité d'activité existe. **4-** Et est testé et mis à jour régulièrement en fonction des changements organisationnels et des risques émergents.	2	• Identifier les moyens techniques, humains et contractuels indispensables pour assurer la continuité de service. • Identifier les dépendances et interconnexions entre les sites.	4	• Le plan de continuité et les modes opératoires de continuité sont formalisés et testés. • Le plan est disponible en format électronique et papier en cas de sinistre.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Avez-vous réfléchi à un plan de reprise des activités (PRA) en cas d'incident majeur ?	**0-** Aucun plan de reprise n'a été prévu. **1-** Le site a réalisé une analyse d'impact en cas de sinistre. **2-** Et le site a identifié les objectifs de reprise des systèmes soutenant les processus métier. **3-** Et un plan de reprise d'activité existe. **4-** Et testé et mis à jour régulièrement en fonction des changements organisationnels et des risques émergents.	2	• Identifier les moyens techniques, humains et contractuels indispensables pour assurer la reprise de service. • Identifier les chaînes de dépendance à prendre en compte lors d'une reprise.	4	• Le plan de reprise et les modes opératoires de continuité sont formalisés et testés. • Le plan est disponible en format électronique et papier en cas de sinistre.
1	Avez-vous mis en place des procédures de sauvegarde de vos données et configurations ?	**0-** Aucune sauvegarde n'est effectuée. **1-** Les systèmes à sauvegarder ont été identifiés. **2-** Et les sauvegardes sont réalisées occasionnellement. **3-** Une procédure de sauvegarde est formalisée et exécutée. **4-** La procédure est contrôlée régulièrement.	2	• Les logiciels, configurations et données associées aux équipements sont sauvegardés à chaque modification. • Une sauvegarde hors site et hors ligne est en place.	4	Un outil dédié de sauvegarde permet d'assurer le suivi du plan de sauvegarde et d'identifier des anomalies.
2	Testez-vous la restauration des données et des configurations que vous avez sauvegardées ?	**0-** Aucun test de restauration n'a été réalisé. **1-** Une procédure générique de restauration du fournisseur est existante. **2-** La restauration des sauvegardes a été réalisée au moins une fois. **3-** Et elle est formalisée à travers une procédure adaptée au système d'informatique industrielle. **4-** La procédure de restauration des sauvegardes est formalisée et testée de façon régulière (<2 ans) sur tous les systèmes. Elle est mise à jour et revue après chaque test.	2	Des tests de restauration sont réalisés au minimum sur un périmètre représentatif des systèmes.	4	• Une procédure de restauration est en place et testée (<2 ans) sur tous les systèmes. • Des modes opératoires de restauration sont rédigés et disponibles. • La procédure doit être mise à jour et revue après chaque test.

10. Audit, contrôle, suivi des indicateurs

- **Analyse de maturité vis à vis du risque cyber :** une analyse du niveau de protection du système d'informatique industrielle doit être menée. Celle-ci apportera une connaissance supplémentaire au système étudié et permettra surtout d'identifier et d'évaluer la menace. Elle servira ensuite pour la mise en place de mesures de sécurité techniques, physiques et organisationnelles adaptées aux risques et aux besoins.

- **Plan de remédiation :** ce plan est basé sur les résultats de l'analyse de maturité et permet de traiter les risques cyber du système industriel. Les responsables du plan seront définis, la réalisation planifiée et les budgets affectés.

- **Contrôle des sociétés tierces :** les intervenants extérieurs peuvent être vecteurs d'une attaque cyber. Ainsi il convient d'engager ces sociétés en imposant formellement la mise en œuvre des moyens organisationnels et techniques pour une bonne sécurité des interventions.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Avez-vous évalué le niveau de maturité de vos installations vis-à-vis du risque cyber ?	**0-** Aucun audit n'est réalisé. **1-** Le niveau de maturité cyber a été auto-évalué, sans vérification. **2-** Le niveau de maturité est vérifié par une visite technique. **3-** Des audits organisationnels d'architecture et de configuration sont réalisés occasionnellement. **4-** Avec une mise à jour après tout changement impactant le système.	1	La conformité des équipements et procédures avec un référentiel adapté (Astee ou autre) est vérifiée initialement et à chaque changement d'exploitant et/ou tous les six ans.	4	• En cas de changement significatif de l'architecture, des équipements, des procédures, ou de l'organisation, une vérification de conformité est réalisée. • Les non-conformités sont documentées et intégrées dans le plan de remédiation.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Avez-vous mis en place un plan d'action pour remédier aux défauts identifiés vis-à-vis de la protection cyber ?	**0-** Aucun plan de remédiation n'est prévu. **1-** Le plan de remédiation est défini. **2-** Et les responsabilités de la mise en œuvre sont identifiées. **3-** Et les dates de réalisation sont programmées et un budget est affecté. **4-** Et la mise en œuvre est suivie.	3	Un plan de remédiation est mis en œuvre.	4	• Un budget est attribué à la réalisation du plan de remédiation. • Un suivi du plan a été mis en place impliquant les acteurs clés.
3	Contrôlez-vous les sociétés tierces avant qu'elles interviennent sur votre infrastructure industrielle ?	**0-** Aucun engagement ni contrôle de la société tierce. **1-** Le site s'appuie sur une déclaration informelle de la société tierce. **2-** La société tierce confirme formellement son niveau d'engagement sécurité et signe un accord de non-divulgation (NDA). **3-** Et fourni des éléments de preuve. **4-** La société tierce complète et signe un PAS (Plan d'Assurance Sécurité) fourni par le demandeur.	2	Les exigences cyber sont présentes dans les contrats.	4	• Un Plan d'Assurance Sécurité, fourni par le demandeur, est complété par la société tierce. • Le demandeur valide le PAS, en acceptant les risques résiduels. • Un suivi du respect du plan d'assurance sécurité est réalisé pour vérifier sa mise en application.
3	Comment est vérifié le niveau de sécurité des réseaux et des configurations de vos équipements ?	**0-** Aucun contrôle de sécurité n'est effectué. **1-** Autocontrôle à partir du référentiel Astee ou autre. **2-** Un audit organisationnel est réalisé par une tierce partie. **3-** Et un audit de configuration et d'architecture est réalisée. **4-** Et des tests d'intrusion sont réalisés.	1	Réalisez un auto-contrôle. Impliquer la totalité des acteurs concernés.	4	Vérifier l'ensemble de votre SI et son organisation avec des audits et tests d'intrusion par un prestataire spécialiste des systèmes industriels.

A. Éléments contractuels

L'analyse des impacts potentiels en cas d'attaque cyber sur les outils techniques et industriels ainsi que l'analyse de la sensibilité d'exposition et de maturité de ces systèmes constituent une étape préalable essentielle à la protection des installations.

La collectivité peut mener elle-même ces réflexions éventuellement avec l'appui de sociétés disposant de l'expertise en ce domaine. Elle peut également choisir de confier cette mission à son exploitant dans le cadre d'une délégation de service public ou d'une prestation de service.

Le contrat d'exploitation devra prévoir l'obligation de mise en place de plans de continuité et de reprise d'activité (PCA/PRA).

Les responsabilités de chaque acteur (collectivité / exploitant) seront définies et une clause de réversibilité en fin de période contractuelle sera prévue en définissant en particulier les biens de retour dans le domaine de la cybersécurité.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Avez-vous défini contractuellement avec votre exploitant les exigences en termes de cybersécurité ?	**0-** Il n'y a pas d'exigences de cybersécurité dans les contrats. **1-** L'exigence de cybersécurité est citée dans le contrat, et une visite technique sur site est organisée. **2-** Le niveau de maturité requis est fourni à l'exploitant selon un référentiel (Astee ou autre). **3-** Les écarts par rapport au référentiel sont qualifiés. **4-** Un plan de remédiation est défini.	2	Intégrer des exigences de cybersécurité dans le contrat de concession/délégation de service public ou de prestation de services.	4	Idem petite structure.
1	Avez-vous défini contractuellement avec votre exploitant les responsabilités de chaque acteur ?	**0-** Aucune prescription en lien avec la cybersécurité. **1-** Un référent cybersécurité est désigné chez le concessionnaire/délégataire de service. **2-** Une grille de rôles et responsabilités a été définie par grandes thématiques. **3-** Les moyens techniques, humains et financiers de chaque partie sont définis. **4-** Une grille détaillée des rôles et responsabilités a été définie.	3	• Définir les responsabilités du délégataire et les moyens techniques, humains et financiers à mettre en œuvre. • Un référent cybersécurité sera désigné chez le concessionnaire/délégataire de service.	4	• Un RACI complet et détaillé clarifie les rôles et responsabilités de chaque partie. • Il est revu et mis à jour régulièrement.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
2	Comment sont gérés et sécurisés les transferts de données entre l'exploitant et la collectivité ?	**0-** Les données sont transférées de manière non-sécurisée. **1-** Les données sont transférées, à la demande, de manière sécurisée. **2-** Les données sont transférées, en discontinu, de manière sécurisée. **3-** Les données sont mises à disposition via une plate-forme dédiée, sécurisée et en discontinu. **4-** Les données sont transmises ou transférées en temps réel via un dispositif sécurisé.	2	• En fonction des besoins de la collectivité, définir une méthode de mise à disposition et de transfert des données intégrant la problématique de cybersécurité. • La sécurisation des données doit respecter les exigences de sécurité liées à l'architecture. • Le mode de transfert et les sécurisations sont définis dans le contrat.	4	Idem petite structure.
1	Avez-vous défini les biens, documents, logiciels et données qui rentreront dans la catégorie des biens de retour (clause de réversibilité) en fin de contrat ? Ceci, en particulier pour tout ce qui concerne la cybersécurité.	**0-** Pas de prescriptions de fin de contrat prévus. **1-** Fourniture par l'exploitant au minimum six mois avant la fin du contrat d'un inventaire détaillé et exhaustif des biens informatiques, physiques ou logiques, et leur appartenance. **2-** L'inventaire comprend l'identification des comptes utilisateur, mots de passe et clés à transférer **3-** Les principaux éléments techniques liés à la cybersécurité sont considérés comme des biens de retour. **4-** Tous les éléments techniques liés à la cybersécurité sont considérés comme des biens de retour.	4	• Dans le contrat, définir les biens, logiciels et données qui rentreront dans la catégorie des biens de retour (clause de réversibilité). Une attention particulière doit être apportée aux outils de cybersécurité tels que les antimalware et les sondes réseau. • Dans le contrat, intégrer des clauses de destruction des données. • Identifier les comptes utilisateur, mots de passe et clés à transférer. • Définir les personnes responsables de vérifier le transfert des biens, logiciels et données à la fin du contrat. • Privilégier le transfert les jours ouvrés en milieu de semaine.	4	Idem petite structure.
2	Comment sont gérées les interventions des fournisseurs de l'exploitant sur le système d'informatique industrielle ?	**0-** Pas de prescriptions sur l'intervention des entreprises tierces intervenantes dans le contrat d'exploitation. **1-** Le contrat d'exploitation prévoit les conditions générales d'accueil des entreprises tierces intervenantes. **2-** Le contrat d'exploitation prévoit un document d'accueil pour les entreprises tierces intervenantes sur site. **3-** Un document d'accueil est effectivement mis en place pour les entreprises tierces intervenantes sur site. **4-** Un document d'accueil existe et une sensibilisation cybersécurité est organisée avant chaque intervention.	2	• Formalisation d'un document d'accueil cybersécurité, adossé au contrat d'exploitation, à destination de tous les intervenants sur site ou lors de maintenances. • Avant chaque intervention, une sensibilisation à la cybersécurité est organisée par l'exploitant.	4	Idem petite structure.

B. Sensibiliser et former le personnel de l'exploitant et de la collectivité

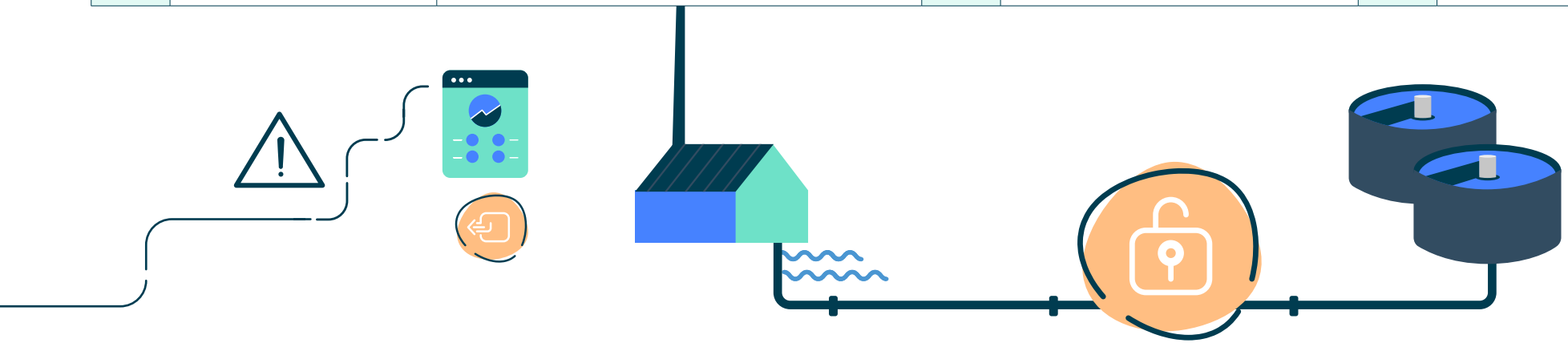
- **Sensibilisation et formation :** le facteur humain étant souvent la porte d'entrée d'une cyber-attaque, il convient de sensibiliser et de former les intervenants aux bonnes pratiques de cybersécurité. Cette sensibilisation aura pour effet de diminuer fortement les négligences largement exploitées par les cyberattaquants. Les avancées technologiques ainsi que les schémas d'attaques évoluant au fil des années, cette sensibilisation devra être suivie dans le temps.

- **Formation aux outils cyber :** une formation aux outils permettant d'assurer la cybersécurité des installations (antivirus, EDR, VPN…) permettra une utilisation dans les règles de l'art. Elle complétera la sensibilisation préalablement réalisée.

- **Compétences cyber interne :** la gestion du risque cyber au sein d'une collectivité nécessite pour son personnel d'étendre ses compétences au volet cyber. Il conviendra à la structure d'identifier les éléments ayant des prédispositions à la cyber, de mettre en place un plan de formation et de la suivre afin que les personnes identifiées conservent un niveau de connaissance dans le temps.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Votre personnel est-il sensibilisé aux bonnes pratiques élémentaires de sécurité et à la notion de résilience ?	**0-** Aucune sensibilisation. **1-** Sensibilisation généraliste réalisée pour l'ensemble du personnel. **2-** Sensibilisation pour chaque nouvel arrivant ou changement de poste. **3-** Sensibilisation adaptée à chaque métier. **4-** Sensibilisation mise à jour régulièrement.	2	• Sensibilisation aux règles de base de la cybersécurité. • Exemples d'éléments à inclure : – Choisir un bon mot de passe. – Reconnaître un mail suspicieux. – Verrouiller son ordinateur. – Ne pas naviguer sur Internet depuis un poste industriel. – Je signale toute activité suspecte. – Ne pas chercher à contourner les dispositifs de sécurité.	4	• Adaptation de la sensibilisation pour les postes à risque. • Organisation d'une réunion régulière autour de la thématique de la cybersécurité (Ex : « le 1/4 d'heure de la sécurité »). • Évaluation des connaissances cyber.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
3	Avez-vous formé votre personnel aux outils de cybersécurité ?	**0-** Aucune formation. **1-** Le personnel a reçu une formation informelle dans l'année précédente. **2-** Formation initiale réalisée avec mise à disposition de documentation (procédures, supports de formation, ...) **3-** Le personnel a reçu une formation avec spécialisations adaptée aux métiers dans l'année précédente. **4-** Formation régulière et connaissances évaluées.	2	Formation sur les outils permettant d'assurer la sécurité informatique dans l'organisation. Ex : filtrage des mails, VPN, antivirus.	4	• Adaptation de la formation pour les postes à risque. • Renouvellement régulier des formations.
1	Comment sont gérées les compétences internes en matière de cybersécurité ?	**0-** Pas de gestion des compétences dans le domaine de la cybersécurité. **1-** Compétences cybersécurité identifiées. **2-** Plan de formation mis en place. **3-** Compétences cybersécurité reconnues dans la structure. **4-** Gestion des postes en fonction des compétences.	2	• Identifier les compétences. • Mettre en place un plan de formation.	4	Gérer les postes en fonction des compétences.



3. Glossaire

TERME	DÉFINITION ANGLAISE	DÉFINITION FRANÇAISE
ANSSI		Agence nationale de la sécurité des systèmes d'information.
API	Application Programming Interface.	Interface logicielle permettant de se connecter avec un équipement d'informatique industrielle afin de le piloter ou d'échanger des données.
AR		Analyse de risque.
Authentification forte	2FA - two-factor authentication ou MFA - multi-factor authentication.	Authentification par deux méthodes différentes, par exemple, PIN et confirmation sur mobile.
Bastion		Serveur d'authentification et de traçage de l'activité.
Biens de retour		Biens matériels ou immatériels qui seront remis au propriétaire des installations à l'issue du contrat d'exploitation.
Cartographie		Document explicitant les informations suivantes : • pour les équipements, dénomination unique, localisation, schéma des flux (matrice), • pour les logiciels, version du système d'exploitation et des applications, ports, • pour les intervenants, rôles et droits.
CERT	Computer emergency response team.	Un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations.
Compte logique		Un compte informatique sécurisé avec un identifiant et mot de passe.
DMZ	Demilitarized Zone.	Zone démilitarisée (zone de réseau public mais protégée).
DSP		Délégation de Service Public / concession de Service Public.
EBIOS		Une méthode d'évaluation des risques cyber, recommandée par l'ANSSI.

TERME	DÉFINITION ANGLAISE	DÉFINITION FRANÇAISE
EDR	Endpoint Detection Response.	Logiciel équivalent aux logiciels antivirus dernière génération basé sur le comportement de l'ordinateur / serveur et capable de réaliser des actions automatiques de remédiation en informant le SOC.
Entité de gestion		Unité homogène de service. En régie il s'agit d'une unité homogène d'exploitation. En DSP il s'agit du périmètre du contrat de délégation.
FW / Firewall	Firewall.	Pare-feu : logiciel de surveillance et de contrôle des applications et des flux de données.
Hardening		Endurcissement (point de vue logique / hardware).
Infogérance		L'infogérance est la prise en charge contractuelle, par un prestataire extérieur, d'une partie ou de la totalité des ressources informatiques d'une entreprise (exploitation ou autres activités).
IT	Information Technology.	Réseaux de gestion, bureautique, basés sur la technologie IP.
LAN	Local Area Network.	Réseau informatique local.
LOG	Logging.	Données enregistrées permettant de tracer les événements.
MCO		Maintien en Conditions Opérationnelles : ensemble des stratégies nécessaires pour garantir que les applications, les infrastructures et les matériels soient disponibles à tout moment.
MCS		Maintien en Conditions de Sécurité (ensemble des stratégies nécessaires pour garantir que les applications, les infrastructures et les matériels fonctionnent de manière sécurisée : patch de sécurité, gestion des vulnérabilités, etc.).
MFA	Multi-factor authentication.	Authentification multifacteur (ex : mot de passe + SMS).
NDA	Non Disclosure Agreement.	Accord de non divulgation.
OT	Operational Technologies.	Informatique industrielle (par exemple : automates programmables).
PA		Point d'Accès au réseau via un routeur (par exemple : bornes wifi ou ports Ethernet).
PAS(I)		Plan d'Assurance Sécurité (informatique).

TERME	DÉFINITION ANGLAISE	DÉFINITION FRANÇAISE
Pentest	Penetration test.	Test d'intrusion des réseaux et des configurations. • Boîte blanche : le pentesteur dispose des informations du système industriel (inventaire, cartographie, configuration, etc.).
PLC	Programmable Logic Controller.	Automate Programmable Industriel (à ne pas confondre avec Application Programming Interface).
PRA/PCA ou DRP/BCP	Disaster Recovery Plans / Business Continuity Plan.	Plan de Reprise d'Activité / Plan de Continuité d'Activité.
Principe de moindre privilège		Les droits d'accès d'un utilisateur sont limités en fonction des tâches qu'il doit réaliser dans le cadre de son travail.
RACI	Responsable Accountable Consulted Informed.	Réalisateur / Approbateur / Contributeur / Informé : rôle et responsabilités pour une tâche identifiée.
Réseau de sûreté physique	Physical security network.	Système d'information lié à la vidéosurveillance, détection d'intrusion, alarmes incendie etc.
SCADA	Supervisory Control and Data Acquisition.	Système de supervision industrielle en temps réel.
SCI / ICS	Industrial Control System.	Système de Contrôle Industriel.
Serveur de rebond	Proxy server.	Serveur situé en DMZ permettant de désactiver/dégrader l'accès à d'autres serveurs/réseaux en cas d'attaque en assurant une rupture protocolaire.
Service d'eau et d'assainissement		Un service public d'eau ou d'assainissement assure la distribution d'eau potable aux abonnés et/ou la collecte et l'épuration des eaux usées.
SFTP	Secure File Transfer Protocol.	Protocole sécurisé de transfert de fichiers.
SIEM	Security Information and Event Management.	Outil centralisé de gestion des événements de sécurité.
SLA	Service Level Agreement.	Accord de niveaux de service : un contrat définissant les différents services qu'un tiers fournira, ainsi que le niveau de service. Par exemple : ouvrir un nouveau flux sur le réseau sous 2 jours.
SOC	Security Operation Center.	Centre d'opérations analysant les événements liés à la sécurité informatique.
VLAN	Virtual LAN.	Réseau virtuel local.
VPN	Virtual Private Network.	Réseau de communication privé.
WAN	Wide Area Network.	Réseau étendu intersite.

4. Proposition de classement des collectivités

Le référentiel différencie deux types de structure. Il revient à chaque collectivité de prendre en compte sa situation en fonction des critères indicatifs ci-dessous pour apprécier la catégorie qui lui correspond le mieux.

TAILLE DE STRUCTURE	TYPE DE COLLECTIVITÉ	TAILLE DE LA COLLECTIVITÉ	MOYENS HUMAINS DE LA COLLECTIVITÉ	DÉGÂTS ENVIRONNEMENTAUX POTENTIELS D'UNE CRISE	COÛT ÉCONOMIQUE POTENTIEL D'UNE CRISE
INTERMÉDIAIRE	Établissement public de coopération intercommunale (E.P.C.I). OU Syndicat intercommunal ayant une structure technique.	> 20 000 habitants	• Gestion s'appuyant sur une équipe technique. • Référent informatique ou agent spécialiste informatique dans la structure.	Risque de rejet dans une rivière classée « très bon état écologique », « réservoir biologique » ou « territoire salmonicole ». OU Dégradation de la qualité des milieux naturels réversible en plus d'une semaine.	100 000 € à plusieurs millions €
PETITE	Communes - Syndicat de communes.	< 20 000 habitants	• Gestion administrative. • Gestion technique limitée.	Pas de risque de rejet dans une rivière classée « très bon état écologique », « réservoir biologique » ou « territoire salmonicole ». ET Dégradation de la qualité des milieux naturels réversible en moins d'une semaine.	< 100 000 €

astee

L'association des professionnels
de l'eau et des déchets

La cybersécurité s'impose aujourd'hui comme un enjeu majeur dans les secteurs de l'eau et de l'assainissement, au cœur de la digitalisation croissante des métiers et de la multiplication des outils numériques. Si ces évolutions sont essentielles pour améliorer la performance des services, elles exposent également les installations à des risques accrus. Entre la gestion des installations – marquée par la multiplication des capteurs, des automates et des accès à distance – et la gestion des données techniques ou personnelles, les vulnérabilités se multiplient.

La sécurité des installations et des systèmes d'information devient ainsi un impératif pour garantir la disponibilité, l'intégrité et la confidentialité des données. De nouveaux risques, tels que les cyberattaques, le rançonnage ou encore les détournements de fonds, doivent être anticipés pour assurer la continuité des services : alimentation en eau potable, traitement des eaux usées et préservation des infrastructures.

Ce guide méthodologique a été conçu pour aider les petites et moyennes collectivités à sécuriser efficacement leurs réseaux d'eau potable et d'assainissement face à ces menaces. Il met en lumière les enjeux de cybersécurité spécifiques à ces infrastructures et présente des bonnes pratiques adaptées aux réalités du terrain. À travers des recommandations claires et opérationnelles, il permettra aux gestionnaires de renforcer leur dispositif de protection et de se conformer aux nouvelles exigences européennes, notamment la directive NIS2, qui étend la réglementation en matière de cybersécurité aux secteurs de l'alimentation en eau et de l'assainissement.

astee.org