Journal officiel
de l'Union européenne

FR
Série C

C/2026/3712

13.7.2026

COMMUNICATION DE LA COMMISSION

Lignes directrices concernant l'application de l'article 13, paragraphe 5, de la directive (UE) 2022/2557 sur la résilience des entités critiques

(C/2026/3712)

I. INTRODUCTION

1. La directive (UE) 2022/2557 sur la résilience des entités critiques ([1]) (ci-après la «directive») vise à faire en sorte que les services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales soient fournis sans entrave dans le marché intérieur. Cette directive a pour but de renforcer la résilience des entités critiques qui fournissent de tels services, en créant un cadre global pour la résilience face à tous les risques (naturels et d'origine humaine, accidentels ou intentionnels).

2. Conformément à l'article 6, paragraphe 1, de la directive, les États membres doivent recenser leurs entités critiques pour les secteurs et sous-secteurs figurant à l'annexe de la directive au plus tard le 17 juillet 2026. Pour assurer un niveau élevé de résilience, la directive établit certaines obligations concernant ces entités critiques, y compris l'obligation prévue à l'article 13 de prendre des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées pour garantir leur résilience. À cet égard, dans l'article 13, paragraphe 5, de la directive, la Commission a été chargée d'adopter des lignes directrices non contraignantes afin de préciser davantage les mesures techniques, les mesures de sécurité et les mesures organisationnelles que peuvent prendre les entités critiques.

3. Conformément aux dispositions susmentionnées, avant l'adoption de la présente communication, les États membres et les parties prenantes ont été consultés lors d'un atelier organisé le 29 septembre 2025. Le groupe sur la résilience des entités critiques (GREC) a été consulté sur les grandes lignes de la communication lors de ses réunions du 10 avril, du 19 mai et du 30 septembre 2025. Il a également été consulté sur le projet de texte de la communication le 14 novembre 2025, et une version mise à jour lui a été transmise le 25 février 2026. Une dernière consultation du GREC sur le projet de lignes directrices a eu lieu le 6 mars 2026.

4. La présente communication n'est pas juridiquement contraignante et n'a pas d'incidence sur l'interprétation du droit de l'Union par la Cour de justice de l'Union européenne.

II. LIGNES DIRECTRICES NON CONTRAIGNANTES SUR LES MESURES DE RENFORCEMENT DE LA RÉSILIENCE

A. CONSIDÉRATIONS GÉNÉRALES

5. Les présentes lignes directrices non contraignantes visent à préciser davantage les mesures techniques, les mesures de sécurité et les mesures organisationnelles que peuvent prendre les entités critiques en vertu de l'article 13, paragraphe 1, points a) à f), de la directive. Cette liste de mesures n'est pas exhaustive et peut être complétée par des mesures supplémentaires.

6. Conformément à l'article 13, paragraphe 1, lorsqu'elles mettent en œuvre ces mesures, les entités critiques doivent tenir compte des éléments suivants:

   a) les informations pertinentes fournies par les États membres sur l'évaluation des risques qu'ils ont réalisée en vertu de l'article 5 de la directive. Les États membres devraient envoyer rapidement à leurs entités critiques des informations succinctes et adaptées. Ces informations peuvent comprendre les rapports visés à l'article 9, paragraphe 3, de la directive, transmis à la Commission au moyen du modèle commun de rapport;

   b) des informations pertinentes sur les résultats de l'évaluation des risques de l'entité critique réalisée en vertu de l'article 12 de la directive. Les entités critiques sont encouragées à appliquer une approche globale en garantissant la continuité du ou des services essentiels qu'elles fournissent au lieu de simplement protéger les infrastructures critiques, ainsi qu'en intégrant les résultats de l'évaluation des risques dans leurs mesures de renforcement de la résilience. Pour consolider les mesures de résilience, les entités critiques devraient envisager de procéder à des évaluations complètes des risques qui vont au-delà de leurs dépendances directes, en tenant compte des aspects transfrontières, sectoriels et systémiques de l'interdépendance.

([1]) Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

7. Conformément à l'article 13, paragraphe 1, de la directive, les mesures que doivent prendre les entités critiques doivent être appropriées et proportionnées. Le caractère approprié et proportionné de ces mesures devrait être évalué par rapport aux résultats des évaluations des risques susmentionnées.

   a) Par «mesures appropriées», on entend des mesures fondées sur les risques ou sur les incidences, efficaces et pertinentes, qui peuvent rendre l'entité critique pleinement résiliente dans la fourniture des services essentiels. Le caractère approprié d'une mesure peut varier d'une entité critique à l'autre en fonction des spécificités de chacune.

   b) Par «mesures proportionnées», on entend des mesures nécessaires et suffisantes qui ne sont pas excessives au regard du niveau de risque et de la gravité de l'incident perturbateur. Les mesures devraient être adaptées aux particularités de l'entité critique concernée et tenir compte d'aspects tels que la nature du ou des services essentiels fournis, la chaîne d'approvisionnement et les interdépendances, le rapport coût-efficacité des mesures, la taille de l'entité et l'incidence géographique des services fournis.

8. Les lignes directrices englobent tous les secteurs couverts par le chapitre III de la directive ([2]). La liste d'exemples non exhaustive peut ne pas s'appliquer de la même manière à tous les secteurs et à tous les types d'infrastructures critiques.

9. Les mesures à prendre dépendront des résultats de l'évaluation des risques de l'État membre et des évaluations des risques des entités critiques.

10. Les mesures de résilience prises par les entités critiques au titre de l'article 13, paragraphe 1, points a) à f), devraient être appliquées sans préjudice des mesures découlant de la législation sectorielle pertinente, et en cohérence avec celles-ci, par exemple la législation mentionnée au considérant 31 de la directive, ainsi que la directive révisée sur la sécurité des réseaux et des systèmes d'information (SRI 2) ([3]), la loi européenne sur le climat ([4]), le règlement sur la préparation aux risques dans le secteur de l'électricité ([5]), le règlement concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel ([6]), la directive relative à la sécurité des opérations pétrolières et gazières en mer ([7]), le cadre de l'UE relatif à la sûreté maritime et portuaire ([8]), le règlement général sur la protection des données (RGPD) ([9]), le règlement relatif à la mise en œuvre du ciel unique européen ([10]), le règlement concernant des règles communes dans le domaine de l'aviation civile ([11]) et le règlement d'exécution établissant les modalités d'exécution des fonctions de réseau de la gestion du trafic aérien ([12]).

([2]) Énergie, transports, santé, eau potable, eaux résiduaires, administration publique, espace, et production, transformation et distribution de denrées alimentaires.

([3]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022, p. 80).

([4]) Règlement (UE) 2021/1119 du Parlement européen et du Conseil du 30 juin 2021 établissant le cadre requis pour parvenir à la neutralité climatique et modifiant les règlements (CE) n° 401/2009 et (UE) 2018/1999 (JO L 243 du 9.7.2021, p. 1), notamment en ce qui concerne l'article 5, relatif au changement climatique.

([5]) Règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE (JO L 158 du 14.6.2019, p. 1), notamment en ce qui concerne les mesures découlant des articles 10 et 11.

([6]) Règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et abrogeant le règlement (UE) n° 994/2010 (JO L 280 du 28.10.2017, p. 1), notamment en ce qui concerne les mesures découlant de l'article 8.

([7]) Directive 2013/30/UE du Parlement européen et du Conseil du 12 juin 2013 relative à la sécurité des opérations pétrolières et gazières en mer et modifiant la directive 2004/35/CE (JO L 178 du 28.6.2013, p. 66), notamment en ce qui concerne les mesures découlant de l'article 3.

([8]) Par exemple, la directive 2005/65/CE relative à l'amélioration de la sûreté des ports et la directive 2002/59/CE relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information.

([9]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (JO L 119 du 4.5.2016, p. 1).

([10]) Règlement (UE) 2024/2803 du Parlement européen et du Conseil du 23 octobre 2024 relatif à la mise en œuvre du ciel unique européen (JO L, 2024/2803, 11.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2803/oj), et notamment son article 22, paragraphe 2, point b).

([11]) Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne (JO L 212 du 22.8.2018, p.1).

([12]) Règlement d'exécution (UE) 2019/123 de la Commission du 24 janvier 2019 établissant les modalités d'exécution des fonctions de réseau de la gestion du trafic aérien (JO L 28 du 31.1.2019, p. 1).

11. Lorsqu'elles utilisent l'intelligence artificielle (IA) dans leurs mesures de résilience (par exemple avec un système d'IA surveillant la pression de l'eau dans un barrage ou contrôlant un réseau électrique), les entités critiques doivent savoir qu'il est impératif, pour les systèmes d'IA à haut risque, de respecter les exigences de sécurité du règlement de l'UE sur l'intelligence artificielle ([13]). Le terme «système d'IA à haut risque» désigne des systèmes destinés à être utilisés en tant que composants de sécurité ([14]) dans le cadre de la gestion et de l'exploitation des infrastructures numériques critiques, du trafic routier et de l'approvisionnement en eau, gaz, électricité et chauffage ([15]). Leur défaillance ou leur mauvais fonctionnement peut mettre en danger la vie et la santé de personnes à grande échelle et entraîner des perturbations importantes dans le déroulement normal des activités sociales et économiques.

12. Lu conjointement avec l'article 13, paragraphe 2, de la directive, le considérant 30 explique que «[d]*ans un souci d'efficacité et de responsabilité, les entités critiques devraient décrire les mesures qu'elles prennent avec un niveau de détail suffisant pour atteindre les objectifs d'efficacité et de responsabilité, eu égard aux risques identifiés, dans un plan de résilience ou dans un ou plusieurs documents équivalents, et appliquer ce plan dans la pratique. Lorsqu'une entité critique a déjà pris des mesures techniques, des mesures de sécurité et des mesures organisationnelles et établi des documents en vertu d'autres actes juridiques qui sont pertinents aux fins des mesures de renforcement de la résilience au titre de la présente directive, elle devrait pouvoir, afin d'éviter les doubles emplois, utiliser ces mesures et documents pour satisfaire aux exigences en ce qui concerne les mesures de résilience au titre de la présente directive* [...].»

13. Le rôle de l'agent de liaison désigné par l'entité critique conformément à l'article 13, paragraphe 3, de la directive est essentiel pour l'adoption et la mise en œuvre efficaces de mesures de renforcement de la résilience, étant donné qu'il garantit une communication et une coordination efficientes et efficaces entre l'entité critique et les autorités compétentes concernant les obligations incombant à l'entité critique ainsi que le cadre de résilience global.

14. Lorsqu'elles prennent des mesures de renforcement de la résilience, les entités critiques sont encouragées à recenser tous les actifs, installations et équipements pertinents et à tenir compte des aspects transfrontières et des éléments d'interdépendance, compte tenu de la nature hautement interconnectée des secteurs couverts par la directive, y compris les aspects physiques, environnementaux, informatiques et liés à la chaîne d'approvisionnement. Toute perturbation dans un certain domaine peut avoir des effets en cascade sur l'ensemble du marché intérieur, compromettant ainsi la fourniture de services essentiels.

15. L'évaluation des risques d'entité critique et l'évaluation des risques nationaux constituent le mécanisme central de prise en considération des interdépendances. Ces évaluations des risques devraient tenir compte de la mesure dans laquelle d'autres secteurs dépendent du service essentiel fourni par l'entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d'autres entités d'autres secteurs, y compris s'il y a lieu, dans les États membres voisins et les pays tiers.

16. Lorsqu'elles prennent des mesures de renforcement de la résilience, les entités critiques devraient prendre en considération les normes internationales et européennes pertinentes.

17. Les particularités des infrastructures maritimes critiques devraient être prises en compte: ces infrastructures sont plus difficiles à surveiller et à protéger; la détection et la localisation des incidents, ainsi que les réparations, prennent plus de temps et coûtent plus cher en mer.

B. MESURES DE PRÉVENTION [article 13, paragraphe 1, point a), de la directive]

18. Les entités critiques sont encouragées à prendre des mesures qui renforcent leur résilience en améliorant leur capacité à prévenir les défaillances ou les perturbations. Ces mesures devraient être intégrées dans le plan de résilience mentionné à l'article 13, paragraphe 2, de la directive et être considérées comme des parties intégrantes d'un système intégré plutôt que comme des composantes isolées. L'efficacité de toute mesure individuelle dépendra de son interaction avec d'autres mesures, y compris la protection physique des locaux, la réaction aux incidents perturbateurs, la résistance à ceux-ci et le rétablissement à la suite de tels incidents, ainsi qu'une gestion adéquate de la sécurité du personnel.

([13]) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([14]) Les composants de sécurité des infrastructures critiques sont des systèmes utilisés pour protéger directement l'intégrité physique des infrastructures critiques ou la santé et la sécurité des personnes et des biens, mais qui ne sont pas nécessaires au fonctionnement du système (article 3, paragraphe 14, et considérant 55 du règlement sur l'intelligence artificielle).

([15]) Voir l'annexe III, point 2, du règlement sur l'intelligence artificielle.

19. Les mesures de réduction des risques de catastrophe et d'adaptation au changement climatique devraient être fondées sur des projections climatiques plausibles couvrant la durée de vie des infrastructures critiques. Les entités critiques sont encouragées: à éviter de placer des infrastructures critiques (par exemple des centres de données ou des sous-stations électriques) dans des zones à haut risque; à prendre des mesures pour renforcer structurellement l'infrastructure en question (par exemple en la protégeant contre les incendies, en assurant sa résistance aux inondations, aux sécheresses et aux explosions, et en assurant leur imperméabilité), ainsi qu'à adopter des mesures non structurelles (par exemple des protocoles de formation et de sécurité) pour prévenir les collisions, les explosions, les déversements de matières dangereuses ou les rayonnements; à trouver des solutions fondées sur la nature, telles que l'intégration d'infrastructures vertes (par exemple des zones humides restaurées pour absorber l'afflux d'eau durant les tempêtes, ou des forêts urbaines pour réduire l'effet d'«îlot de chaleur» sur les équipements électriques); à prendre en considération les changements immédiats et à long terme des modèles climatiques qui pourraient dégrader l'intégrité du système au fil du temps, tels que les épisodes de chaleur extrême, les inondations et l'élévation du niveau de la mer; à anticiper les pénuries d'eau; à effectuer des tests de résistance pour s'assurer que l'entité peut fonctionner dans un environnement nettement plus défavorable (par exemple des conditions plus chaudes, plus froides, plus humides, plus sèches, erratiques ou inhabituelles pour la saison).

20. Les entités critiques sont encouragées à envisager de créer une base de données des incidents, d'alimenter les bases de données de l'UE sur les incidents ([16]) et de mettre en œuvre un dispositif systématique de signalement des incidents, qui permettrait d'obtenir un historique des événements et d'assurer non seulement la prévention des incidents et la réduction des risques, mais aussi le recouvrement des avoirs.

21. En vue de prévenir les erreurs humaines, les entités critiques sont encouragées à recenser les tâches pouvant donner lieu à des erreurs ainsi qu'à appliquer des contre-mesures appropriées, y compris pour les tâches liées à l'automatisation, à la formation continue des employés, à la surveillance et à l'établissement de responsabilités claires, à la documentation détaillée des processus, à la réalisation d'audits et d'inspections réguliers, ainsi qu'au développement d'une culture de la résilience et de la responsabilité.

22. Pour veiller à ce que les mesures de résilience soient appliquées de façon conforme à la directive SRI 2, les entités critiques sont encouragées, lorsqu'elles appliquent leurs mesures de résilience, à prendre en considération des mesures pertinentes pour la sécurité des réseaux et des systèmes d'information, telles que définies dans la directive SRI 2. Les mesures énoncées dans le règlement d'exécution (UE) 2024/2690 de la Commission ([17]) applicables à certains types d'entités dans les secteurs de l'infrastructure numérique, de la gestion des services TIC (interentreprises) et des fournisseurs numériques définis dans la directive SRI 2 ([18]), ainsi que les orientations de mise en œuvre formulées par l'Agence de l'Union européenne pour la cybersécurité (ENISA) qui accompagnent ces mesures ([19]), peuvent servir de références supplémentaires.

23. En ce qui concerne la technologie opérationnelle, les entités critiques devraient intégrer des commandes manuelles de secours et des dispositions garantissant que l'humain intervient dans le processus, qui définissent les conditions et exigences spécifiques de l'intervention humaine et du contrôle manuel en réponse aux dangers.

C. MESURES DE PROTECTION PHYSIQUE [article 13, paragraphe 1, point b), de la directive]

24. Les entités critiques sont encouragées à prendre des mesures physiques contre les menaces naturelles et d'origine humaine (par exemple les menaces hybrides, le sabotage, le terrorisme, les actes criminels, le ciblage militaire/en temps de guerre, l'espionnage) et à mettre en place des contrôles procéduraux permettant de détecter, de décourager, de retarder et de bloquer les incidents perturbateurs ainsi que d'y réagir et d'en réduire les effets.

([16]) Dans le domaine de l'aviation, les bases de données pertinentes de l'UE sur les incidents comprennent le système de notification des incidents de l'Agence de l'Union européenne pour la sécurité aérienne, les registres des incidents des gestionnaires de réseaux et le système de notification des événements liés à la sûreté de l'aviation.

([17]) Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance (JO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

([18]) Conformément à l'article 8 de la directive sur la résilience des entités critiques, les États membres veillent à ce que certaines dispositions de la directive, y compris l'article 13, ne s'appliquent pas aux entités critiques qu'ils ont recensées dans certains secteurs, y compris celui des infrastructures numériques. Les États membres peuvent adopter ou maintenir des dispositions de droit national afin d'atteindre un niveau de résilience plus élevé pour ces entités critiques à condition que ces dispositions soient compatibles avec le droit de l'Union applicable. La gestion des services TIC (interentreprises) et le secteur des fournisseurs numériques ne font pas partie des secteurs répertoriés dans l'annexe de la directive.

([19]) https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

25. Lorsqu'elles planifient des mesures appropriées et proportionnées de renforcement de la résilience contre les menaces d'origine humaine, les entités critiques devraient tenir compte de la pertinence de certains scénarios de menace. En particulier, elles sont encouragées à:

    i) prendre en considération la nécessité d'établir des protocoles de coordination étroite entre les secteurs public et privé pour faciliter la coopération opérationnelle avec les autorités compétentes et garantir une transmission appropriée et réciproque d'informations sur les menaces et les incidents, aux fins d'une appréciation commune de la situation;

    ii) dans le cas de menaces hybrides potentielles émanant d'acteurs étatiques qui, en ce qui concerne les entités critiques, sont principalement des tentatives de sabotage visant à endommager des biens et des équipements, ou des préparatifs en vue de telles tentatives (y compris l'espionnage/la surveillance), envisager la possibilité que des acteurs étatiques parrainent et commandent des mandataires vulnérables ou exploitables (par exemple des individus ou des groupes) pour atteindre leurs objectifs, et la possibilité que des acteurs étatiques se livrent à des attaques coordonnées au moyen de vecteurs d'attaque multiples dans plusieurs domaines et/ou en utilisant plusieurs mandataires;

    iii) tenir compte d'autres menaces potentielles, notamment celles découlant du terrorisme et de l'extrémisme violent, des activités criminelles, du ciblage militaire, des menaces internes, de l'activisme, etc.

26. Les entités critiques sont encouragées à envisager des mesures de durcissement du périmètre (dissuasion et retardement), telles que des clôtures de haute sécurité (par exemple impossibles à escalader/sectionner), des murs renforcés, des portails, des entraves à la progression des véhicules hostiles, ainsi qu'une signalisation et un éclairage adéquats (par exemple des avertissements bien visibles pour décourager les intrus opportunistes, et un éclairage de sécurité pour éliminer les zones de non-visibilité à des fins de surveillance).

27. L'accès des véhicules, du personnel et des marchandises aux locaux concernés devrait comprendre un nombre limité de points de passage contrôlables. Les voies d'approche directe des véhicules devraient être limitées par une combinaison d'obstacles physiques (par exemple des bornes fixes et rétractables, des obstacles naturels ou d'autres mesures de limitation de la vitesse), et l'espacement maximal prescrit entre deux obstacles devrait être respecté afin d'empêcher tout contournement par un véhicule.

28. Les points d'entrée extérieurs (par exemple les portes et les portails) des locaux concernés devraient avoir une structure robuste ou renforcée, et être équipés (après leur installation, si nécessaire) de charnières et de mécanismes de verrouillage sécurisés. Les encadrements des ouvertures des installations (par exemple les fenêtres et les fenêtres de toit) devraient également être équipés (après leur installation, si nécessaire) de mécanismes de verrouillage et de couches protectrices (par exemple barreaux, grilles, vitres résistantes aux chocs, membranes protectrices). Les points d'entrée non conventionnels (par exemple les trappes de toit, les regards et les évents) des installations ou des biens devraient également être protégés contre toute ouverture ou manipulation non autorisée.

29. Les entités critiques sont encouragées à envisager des moyens de surveillance et de détection au niveau du périmètre afin de détecter toute intrusion en temps réel (par exemple l'installation d'alarmes ou de systèmes de détection des intrusions, y compris des capteurs intérieurs et extérieurs). Ces dispositifs devraient assurer une couverture adéquate de la zone, être soumis à des protocoles de surveillance et d'intervention cohérents et faire l'objet de tests fonctionnels réguliers. Les détections d'accès légitimes, les défaillances du système et les fausses identifications positives devraient être analysées et des mesures correctives devraient être mises en œuvre pour préserver l'intégrité de l'installation.

30. Les entités critiques sont encouragées à faire en sorte que les systèmes vidéo fournissent une couverture en temps réel, enregistrée, claire et spécifique à l'environnement des biens, installations et équipements pertinents, ainsi que des voies d'approche et des points d'entrée des locaux. La synchronisation temporelle, l'état d'enregistrement et les périodes de conservation des données de surveillance devraient être vérifiés régulièrement. Les entités devraient procéder à des contrôles d'enregistrement de routine afin de confirmer que les visages, les actions et les événements sont identifiables aux fins médico-légales prévues en cas d'incident. Des composants critiques de rechange (par exemple des supports de mémoire, des groupes électrogènes) doivent être conservés proportionnellement aux besoins.

31. Les entités critiques sont encouragées à faire en sorte que les dispositifs d'éclairage assurent un éclairage uniforme des entrées, des zones de stationnement, des allées et des champs de vision des caméras, en évitant tout éblouissement et toute ombre profonde qui pourraient entraver la détection ou l'enregistrement. Les éclairages de secours et de remplacement devraient être testés régulièrement. Des mesures correctives (par exemple le remplacement des ampoules, l'ajustement de la couverture, l'élagage de la végétation) devraient être appliquées régulièrement.

32. La signalétique doit indiquer clairement les restrictions de sécurité, les mentions relatives à la surveillance et à la confidentialité, ainsi que les voies réservées au personnel, aux visiteurs et aux livraisons.

33. Les entités critiques sont encouragées à envisager des mesures de contrôle de l'accès (avec possibilité de refus) à l'aide de zones de sécurité à plusieurs niveaux, de dispositifs de gestion des accès physiques (par exemple lecteurs de badges, scanners biométriques), de portillons et de portes à verrouillage successif. Le recours à des agents de sécurité présents sur place pour patrouiller et gérer le contrôle d'accès aux installations, points d'entrée ou équipements pertinents devrait être envisagé. Le personnel de sécurité devrait également assurer une fonction d'intervention en cas d'incident. Il devrait entretenir des contacts étroits et réguliers avec les autorités répressives et les acteurs de la défense concernés.

34. Les salles et les enceintes abritant des infrastructures ou équipements d'électricité, d'eau, de gaz, de chauffage, de ventilation, de climatisation, de télécommunications, de sécurité, de réseau ou d'autres infrastructures ou équipements sensibles devraient être verrouillés et leur accès devrait être contrôlé. Il convient en outre de prévoir des mesures proportionnées visant à empêcher l'ouverture et la manipulation non autorisées de ces infrastructures et équipements.

35. Les salles de courrier et les dépôts de livraison devraient être situés à l'écart des biens, des installations, des équipements pertinents et des zones très fréquentées, et être équipés de manière à permettre la mise à l'écart et l'inspection sécurisée des objets potentiellement suspects. Des procédures claires devraient être communiquées au personnel pour le traitement des objets suspects, notamment en matière d'isolement, de désescalade et de notification aux parties prenantes internes et externes concernées. Des outils d'ouverture et des équipements de protection individuelle devraient être mis à disposition si nécessaire. La chaîne de contrôle des livraisons de valeur ou contrôlées devrait être documentée de la réception au destinataire. Des contrôles ponctuels devraient être effectués et enregistrés à intervalles réguliers.

36. Tous les biens, installations ou équipements extérieurs devraient également faire l'objet de mesures de protection proportionnées. Toute mesure de protection physique prise par les entités critiques doit être accompagnée d'inspections et de mesures de maintenance régulières.

37. Les mesures relatives aux contrôles de l'accès du personnel et à la sécurité physique des informations sensibles ou classifiées n'invalident pas les obligations en matière de gestion des risques liées à la cybersécurité énoncées dans la directive SRI 2 ([20]).

38. Outre les orientations concernant la gestion de la sécurité du personnel figurant dans la partie F des présentes lignes directrices, les entités critiques sont encouragées à tenir un registre unique faisant autorité répertoriant les clés physiques et des justificatifs d'identité (électroniques), y compris leurs dates de délivrance, de révocation et de restitution. Les clés ou justificatifs d'identité perdus ou volés devraient être révoqués immédiatement et les serrures devraient être changées ou remplacées en cas de suspicion de compromission.

39. Les entités critiques sont encouragées à veiller à ce que les droits d'accès respectent le principe du «moindre privilège» et soient réexaminés régulièrement ou lors de tout changement de fonction. Les espaces pertinents devraient être divisés en différentes zones, contrôlées par des mesures correspondant concernant certains types de personnes (par ex. distinguer les zones publiques, les zones de travail, les zones restreintes et les zones critiques) et combinant des contrôles physiques, techniques et administratifs. Tout accès devrait être enregistré. Les visiteurs devraient être conduits jusqu'à un point de passage contrôlé, enregistrés, munis d'une identification visible et escortés au-delà de la réception, sauf autorisation contraire. Ces moyens d'identification devraient être immédiatement désactivés à la fin de leur visite. Les procédures correspondantes devraient être simples, documentées et communiquées à l'ensemble du personnel, en particulier au personnel chargé de l'accueil et de la sécurité.

40. Toute ressource d'information sensible devrait être positionnée, protégée et stockée de manière à réduire les risques pour son intégrité (par ex. visualisation non autorisée ou accidentelle, manipulation, vol, dommages environnementaux), et accessible selon le principe du «besoin d'en connaître».

41. Les entités critiques sont encouragées à établir et à tenir à jour un inventaire et/ou un répertoire des ressources d'information sensibles. Ces ressources devraient être classées en fonction du niveau de sensibilité de l'activité qui leur est associée ou du niveau de sécurité à assurer. Les entités devraient ensuite utiliser un système pour documenter les ressources d'information (par ex. information restreinte, interne, publique ou équivalents), et étiqueter et manipuler ces ressources en conséquence. Les règles et procédures de classification et de manipulation devraient être communiquées à l'ensemble du personnel concerné et faire l'objet d'un réexamen périodique. Ces règles comporteront notamment des instructions relatives à l'accès des bureaux et des écrans aux informations et à la création ou à la copie d'informations.

([20]) Article 21.

42. Le cas échéant, les entités critiques devraient garder à l'esprit les règles nationales applicables en matière de protection des informations classifiées jugées pertinentes pour la sécurité nationale.

43. Si certaines parties prenantes externes ont besoin d'accéder à des actifs informationnels, les entités critiques sont encouragées à envisager l'élaboration d'orientations à l'intention des utilisateurs et des accords de non-divulgation, ou d'autres mécanismes contractuels pertinents, le cas échéant.

44. Toutes les installations hébergeant des ressources d'information sensibles (par ex. archives, salles de serveurs) ou d'autres zones à partir desquelles des ressources d'information sensibles pourraient être extraites devraient être désignées et surveillées en tant que zones sécurisées, avec des contrôles particulièrement stricts en matière d'accès, de consultation et de retrait.

45. Les entités critiques devraient veiller à ce que les droits d'accès soient régulièrement examinés et revus. Des durées de conservation devraient être définies pour les ressources d'information sensibles. Une fois que ces délais ont été dépassés ou que d'autres évolutions nécessitent un reclassement des actifs informationnels, des mesures appropriées devraient être prises pour assainir ou détruire ces actifs.

46. En ce qui concerne les menaces posées par les systèmes sans pilote ([21]) (drones), les entités critiques sont encouragées à mettre en œuvre des mesures visant à faciliter la détection, le suivi et l'identification de tels systèmes (par ex. radars, détecteurs de radiofréquences, caméras de surveillance thermique/de jour, capteurs acoustiques). Dans la mesure du possible, les entités critiques devraient également coopérer avec les fournisseurs de services de télécommunications afin d'obtenir l'accès aux données générées par les technologies de détection et de communication intégrées (ISAC), en vue de détecter toute activité non autorisée de drones dans leur périmètre de sécurité.

47. Il convient de réduire le risque d'espionnage/de surveillance par des systèmes sans pilote non coopératifs en atténuant la visibilité (aérienne, maritime ou terrestre) des moyens ou équipements sensibles (par ex. dissimulation ou repositionnement) et, le cas échéant, en veillant à ce que ces moyens ou équipements soient entreposés dans des installations fermées.

48. Les entités critiques devraient également atténuer le risque de sabotage d'installations, de biens ou d'équipements par des systèmes sans pilote non coopératifs. Parmi les exemples de telles mesures d'atténuation figurent les filets ou les voilures antidrones ainsi que d'autres mesures de renforcement structurel, comme des fenêtres résistantes aux explosions, le renforcement des dalles de toiture ou la construction d'enclos entièrement fermés.

49. Les entités critiques peuvent envisager d'utiliser certaines zones géographiques pour gérer et atténuer les risques liés à l'exploitation de drones non autorisée ou dangereuse à proximité de leurs locaux. Toute décision d'établir de telles zones devrait faire l'objet d'une évaluation des risques et de la proportionnalité effectuée au cas par cas, compte tenu de la sensibilité potentielle des informations risquant d'être révélées par la publication de données géographiques relatives aux entités critiques. Pour ce faire, les entités devraient coopérer avec les autorités nationales compétentes pour faire en sorte que les zones géographiques concernées soient dûment délimitées et les informations connexes publiées sous forme numérique conformément au cadre applicable dans le domaine de l'aviation. Ces zones devraient, au minimum, permettre aux exploitants de drones d'utiliser des fonctionnalités de géovigilance. Suivant l'évolution des capacités techniques, et lorsque le cadre réglementaire le permet, les entités critiques peuvent également envisager d'utiliser progressivement des fonctionnalités de géorepérage. Le géorepérage peut servir de garantie préventive en réduisant la probabilité d'incursions involontaires de drones conformes dans des zones sensibles. Les entités critiques devraient maintenir un lien opérationnel direct avec le gestionnaire de la zone géographique. Cela leur permettrait de visualiser en temps utile les activités de drones autorisées ou non autorisées à proximité ainsi que de faciliter l'analyse de la situation et la coordination avec les autorités compétentes.

50. Il est essentiel de renforcer les partenariats et la communication avec les opérateurs antidrones des autorités répressives locales et de la défense, ou avec d'autres acteurs disposant d'un mandat légal et de capacités d'atténuation (par ex. brouillage des radiofréquences, usurpation et autres mesures cinétiques ou non cinétiques). À cet effet, les entités critiques sont encouragées à faciliter l'utilisation de systèmes antidrones pour protéger leur périmètre, conformément au cadre juridique applicable.

([21]) Communication (COM)2026 81 final de la Commission du 11 février 2026 concernant un plan d'action relatif à la sûreté des drones et des systèmes antidrones.

D. MESURES D'INTERVENTION, DE RÉSISTANCE ET D'ATTÉNUATION [article 13, paragraphe 1, point c), de la directive]

51. Les entités critiques sont encouragées à envisager les mesures suivantes pour atténuer les conséquences des incidents.

a) Gestion hors site des crises et des catastrophes: mesures visant à atténuer les conséquences négatives hors site d'un incident perturbateur grave et à en informer rapidement les autorités chargées de la gestion des crises et des catastrophes afin de permettre le déploiement de mesures de protection hors site. Une telle démarche nécessite une coordination étroite avec les autorités compétentes, la mise en place de canaux de communication éprouvés, ainsi que des exercices réguliers de gestion des crises et des catastrophes.

b) Assistance hors site: mesures visant à intégrer efficacement l'assistance hors site dans les mesures d'intervention sur site (y compris la gestion des accidents graves, les mesures d'atténuation et l'intervention d'urgence).

c) Concevoir les infrastructures de manière à en préserver la sûreté en cas de défaillance, pour éviter qu'une perturbation ne compromette la sécurité des personnes (y compris celle du personnel) et atténuer les incidences en cascade sur d'autres actifs. Les caractéristiques de sûreté en cas de défaillance permettent à l'infrastructure de maintenir des fonctions essentielles en cas de défaillance ou de prendre en charge des procédures d'arrêt contrôlé qui préviennent les dommages aux équipements et garantissent sa capacité de redémarrage lorsque les conditions le permettent. Il est possible de maintenir des conditions vitales critiques ou une capacité de survie passive grâce à une capacité de stockage adéquate, à un contrôle de la capacité thermique, à un approvisionnement de secours approprié et à des mesures assurant la sûreté des matières dangereuses.

52. Lors de la conception d'infrastructures sûres en cas de défaillance, les entités critiques sont encouragées à prendre en considération les éléments suivants: la capacité de stockage nécessaire dans les scénarios de défaillance les plus défavorables pour maintenir des conditions vitales critiques; l'approvisionnement de secours nécessaire pour maintenir les opérations critiques et permettre l'arrêt contrôlé des opérations de l'infrastructure; la sécurité de toutes les matières dangereuses stockées ou présentes dans les infrastructures critiques, en veillant à ce qu'elles soient incluses dans les plans de codification et de gestion des matières dangereuses et dûment sécurisées en cas de défaillance des infrastructures; des mesures de sécurité thermique pour les actifs des infrastructures critiques hébergeant du personnel ou des équipements sensibles à la température. Ces mesures peuvent porter sur la capacité de chauffage et de refroidissement afin d'éviter des pertes dues à des températures extrêmes lors de perturbations prolongées.

53. Les entités critiques sont encouragées à prendre des mesures pour garantir la disponibilité, l'entretien et les capacités de réparation, ainsi qu'à définir clairement leurs besoins d'approvisionnement, à diversifier leurs sources d'approvisionnement en prévoyant d'autres fournisseurs et itinéraires, à procéder au renforcement des infrastructures, à assurer les redondances et à mettre en place des systèmes de secours assortis de spécifications correspondant aux fonctions, aux durées et aux priorités de restauration.

54. Les entités critiques sont encouragées à prendre des mesures appropriées pour garantir l'intégrité des réseaux et systèmes informatiques et des logiciels utilisés dans les équipements, notamment en ce qui concerne la dépendance à l'égard de fournisseurs à haut risque et la protection contre les interférences dues aux signaux de radiofréquences et aux cyberattaques.

55. Les systèmes d'alimentation électrique de secours peuvent comprendre des générateurs et des batteries d'alimentation sans interruption (ASI). Les systèmes de secours devraient être testés périodiquement; l'autonomie en matière d'alimentation électrique devrait être assurée pendant au moins 72 heures et des contrats avec des fournisseurs devraient être activés pour l'aide d'urgence (approvisionnement, interventions et réparations).

56. Quant à la résilience en matière d'approvisionnement en eau, les entités critiques peuvent limiter l'utilisation de l'eau aux fonctions critiques en cas de perturbations et utiliser d'autres sources, y compris des puits de secours, des réservoirs de stockage, des unités de traitement portables et des options de stockage flexibles. Les entités critiques du secteur de l'eau potable sont encouragées à recenser les points de livraison prioritaires, afin de garantir une réponse adéquate en cas d'urgence ou d'interruption de l'approvisionnement. Lorsqu'elles prennent des mesures de résilience, les entités critiques doivent veiller à ce que les eaux destinées à la consommation humaine respectent les normes de qualité énoncées dans la directive (UE) 2020/2184 ([22]).

([22]) Directive (UE) 2020/2184 du Parlement européen et du Conseil du 16 décembre 2020 relative à la qualité des eaux destinées à la consommation humaine (refonte) (JO L 435 du 23.12.2020, p. 1).

57. Pour d'autres services d'utilité publique (par ex. eau chaude, eau glacée, chaudière à vapeur) et d'approvisionnements sectoriels (par ex. produits chimiques, matières premières, pièces détachées), il conviendrait d'envisager, lors de la planification des mesures d'urgence dans les chaînes d'approvisionnement, une transition des modèles d'inventaire «juste à temps» à des modèles d'inventaire «au cas où», lorsque cela s'avère pertinent. Les systèmes de secours devraient inclure des ressources et des fournitures de secours préétablies (réserves et stocks de sécurité/d'urgence).

58. Les entités critiques sont encouragées à élaborer des programmes de maintenance complets, fondés sur les recommandations des fabricants, sur leur propre expérience opérationnelle et sur les évaluations des risques. La maintenance prédictive peut être appliquée à l'aide de technologies de surveillance avancées comprenant des réseaux de capteurs intégrés. Une maintenance régulière et prédictive fondée sur les performances, qui utilise des outils d'analyse de données et d'IA pour surveiller le vieillissement et prévoir les défaillances, pourrait être appropriée pour optimiser le calendrier de toute intervention requise. Des protocoles clairs devraient être établis pour répondre aux alertes du système de suivi, y compris en ce qui concerne la vérification des alertes, l'évaluation de l'urgence et la mobilisation des ressources de maintenance. Ces protocoles devraient définir des procédures d'intervention par paliers correspondant aux situations qui requièrent une attention immédiate. Des inspections régulières des infrastructures compléteront la surveillance automatisée.

59. En ce qui concerne la gouvernance, les entités critiques devraient considérer que la résilience doit être intégrée du niveau le plus élevé au niveau le plus bas de la structure de gouvernance. Elles devraient établir des objectifs en matière de résilience et adopter une stratégie, une politique et des plans à cet égard, les communiquer aux parties concernées sur la base du besoin d'en connaître et réviser régulièrement ces instruments. Il convient de prendre en considération toute vulnérabilité existante et de déterminer comment mieux prévenir tout incident, s'en protéger, y réagir, y résister, l'atténuer, l'absorber, s'y adapter et s'en rétablir.

60. Les entités critiques sont encouragées à hiérarchiser clairement la prise de décisions. Les compétences nécessaires à la résilience devraient être consolidées au niveau du conseil d'administration ainsi que dans les fonctions de résilience ou de gestion des risques afin de garantir une stratégie, une politique et des plans d'exploitation adéquats en matière de résilience. Les entités critiques sont encouragées à envisager de nommer une personne responsable de la résilience et d'assurer la délimitation claire des rôles et responsabilités de coordination en vue de la réalisation des objectifs de résilience.

61. La mise en place et la formalisation d'une coopération avec les autorités publiques compétentes, y compris les responsables politiques, les services répressifs, les services d'urgence et les acteurs de la défense, sont également pertinentes dans ce contexte. Les entités critiques sont encouragées à clarifier les rôles et les procédures en matière de partage d'informations, de notification et de coordination en réponse aux incidents, ainsi que les attentes de toutes les parties.

62. La mise en place et la formalisation d'une coopération avec les acteurs du secteur privé concernés par le domaine d'activité de l'entité, ainsi qu'avec ceux d'autres secteurs et d'autres États membres, peuvent également être envisagées.

63. Des protocoles de communication de crise devraient être établis afin de garantir un flux d'informations opportun et précis vers les parties prenantes internes et externes (y compris les clients et le public) pendant les incidents. Les entités critiques devraient maintenir des modèles de communication préalablement approuvés, des procédures de notification des parties prenantes et des capacités de communication reposant sur plusieurs canaux, y compris des systèmes redondants. Les communications devraient être adaptées à différents publics, notamment dans plusieurs langues, le cas échéant, et compte tenu des exigences en matière d'accessibilité.

64. La conception de redondances à plusieurs échelles garantit que les services peuvent être fournis aux niveaux transfrontalier, national, régional et local et sont effectivement interopérables.

65. Les entités critiques sont encouragées à faire en sorte que les procédures d'intervention d'urgence comprennent des systèmes d'alerte multicanaux dotés de capacités de géociblage, tels que le service d'alerte d'urgence par satellite du programme Galileo, ainsi que des chaînes de commandement claires en matière de communication, y compris des porte-parole désignés, et des procédures opérationnelles permanentes (POP) adaptées aux risques propres à chaque site. Les entités critiques devraient assurer la maintenance des équipements d'urgence, constituer et former des équipes d'intervention d'urgence, et veiller à ce que les procédures d'évacuation soient accessibles et régulièrement mises en pratique.

E. MESURES DE RÉTABLISSEMENT [article 13, paragraphe 1, point d), de la directive]

66. Pour assurer la continuité des activités, les entités critiques sont encouragées à envisager des mesures de redondance garantissant que les services essentiels continueront d'être fournis en cas de défaillance des systèmes primaires. Ces mesures peuvent comprendre la détermination des sous-services les plus critiques, qui seront les premiers à être rétablis (hiérarchisation des services), le maintien de la capacité à faire fonctionner le matériel manuellement en cas de défaillance ou de manipulation des systèmes automatisés ou fondés sur l'IA, et le rétablissement de la main-d'œuvre en cas d'incident perturbateur.

67. Les autres sites envisageables pour le rétablissement après sinistre peuvent être des sites de secours immédiat (entièrement équipés pour une utilisation immédiate), des sites de secours intermédiaire (partiellement équipés) ou des «sites froids» (qui doivent être configurés suivant la perturbation). Les sites de secours devraient être suffisamment éloignés des installations primaires, tout en restant accessibles. Dans la mesure du possible, des installations mobiles (par ex. des postes de commande centralisée) devraient être envisagées. Les sauvegardes doivent être stockées dans des lieux physiquement séparés ou isolés sur le plan logistique.

68. Sans préjudice de la directive SRI 2 ([23]), les entités critiques devraient élaborer et tenir à jour des plans complets de continuité des activités (PCA), fondés sur des évaluations des incidences sur les activités qui recensent les fonctions critiques, établissent les priorités de rétablissement et définissent des objectifs de temps de reprise (OTR) ainsi que des objectifs de points de reprise (OPR), y compris la mise en place d'accords de niveau de service (ANS). Les PCA devraient préciser clairement les critères d'activation, l'affectation des ressources, ainsi que les rôles et les mécanismes de coordination pour les phases de réaction, de rétablissement, de reprise et de restauration. Ils devraient être mis à l'épreuve, révisés et mis à jour à intervalles planifiés et à la suite de tout incident important ou de toute modification des activités.

69. Les procédures de gestion des crises devraient inclure des structures de commandement en cas d'incident comprenant une autorité décisionnelle clairement définie et des plans d'action documentés en réponse aux incidents. Les entités critiques devraient envisager de mettre en place des équipes de crise dotées de rôles prédéfinis, de protocoles de remontée de l'information, de formations appropriées et de canaux de communication (primaires et de secours) afin de garantir des interventions rapides et coordonnées en cas d'incident perturbateur.

70. La planification des effectifs devrait répondre aux besoins en matière de capacités d'intensification au moyen d'une liste d'effectifs de renfort, de programmes de formation et d'accords d'aide mutuelle préétablis avec les organisations partenaires. Les entités critiques devraient élaborer des cadres de compétences et des plans de succession afin de garantir un niveau suffisant concernant les rôles critiques et de préserver la capacité opérationnelle en cas de perturbations prolongées ou de pénuries de personnel.

71. Pour permettre un rétablissement efficace après un incident, les entités critiques devraient mettre en œuvre des protocoles de redémarrage progressif qui prévoient en priorité la restauration des fonctions critiques sur la base des conclusions de l'évaluation des risques ou de l'évaluation des incidences sur les activités. Ces protocoles devraient comprendre des procédures de validation systématique pour les systèmes critiques, des tests complets de l'intégrité et de la fonctionnalité des données, des mesures de contrôle de la qualité et une transition contrôlée du fonctionnement d'urgence au fonctionnement normal grâce à des augmentations progressives des capacités et à un suivi des performances.

72. Les enquêtes post-incident devraient être fondées sur des méthodes structurées, telles que l'analyse des causes profondes, pour identifier les causes systémiques plutôt que les symptômes immédiats. Des analyses après action devraient être menées à la suite de tous les exercices et incidents réels pour permettre d'en tirer des enseignements; les conclusions devraient être systématiquement consignées et intégrées dans les procédures, les programmes de formation et les évaluations des risques mis à jour afin d'éviter que les incidents ne se reproduisent et de renforcer la résilience de l'organisation.

73. En ce qui concerne les chaînes d'approvisionnement, la résilience est essentielle dans le contexte du rétablissement à la suite d'incidents perturbateurs. Conformément à leurs évaluations des risques, les entités critiques devraient envisager de cartographier la chaîne d'approvisionnement nécessaire à la fourniture de leurs services essentiels, d'élaborer des stratégies de résilience à long terme de cette chaîne d'approvisionnement et de réviser et mettre à jour régulièrement le plan d'urgence relatif à la chaîne d'approvisionnement. Elles sont encouragées à recenser d'autres chaînes d'approvisionnement utilisables en cas d'incidents perturbateurs touchant leur(s) fournisseur(s) clé(s).

([23]) En particulier l'article 21, paragraphe 2, point c), de la directive SRI 2.

74. Les entités critiques devraient envisager la constitution de stocks stratégiques, y compris de stocks de sécurité, de mécanismes de réapprovisionnement rapide et de stockage hors site protégés contre les menaces communes, de sorte que les services essentiels ne soient pas interrompus en cas de perturbation de la chaîne d'approvisionnement.

75. Il serait également judicieux d'envisager la conclusion de contrats formels avec d'autres entités du même secteur pour assurer le partage de ressources, d'équipements ou de personnel dans le cadre d'un effort de rétablissement à grande échelle.

F. MESURES DE GESTION DE LA SÉCURITÉ LIÉE AU PERSONNEL [article 13, paragraphe 1, point e), de la directive]

76. Les menaces liées au personnel devraient être évaluées et traitées de manière à atténuer le risque d'erreur humaine, de sabotage et de menaces internes ainsi que le risque d'absence pour cause de maladie, d'urgence ou de menaces extérieures. Les entités critiques sont encouragées à recenser et à établir des listes de catégories de personnel exerçant des fonctions critiques, en y incluant le personnel des prestataires de services externes (contractants et sous-traitants).

77. En établissant ces listes, elles devraient tenir compte des particularités des services essentiels fournis et relier ces services au personnel participant à leur prestation. À cette fin, les entités critiques devraient conserver une documentation claire, complète et à jour concernant ces catégories de personnel.

78. Outre les considérations susmentionnées concernant les droits d'accès, les entités critiques sont encouragées à définir qui peut accéder aux locaux, aux infrastructures critiques et aux informations sensibles et à quelles conditions. Des procédures efficaces d'octroi et de révocation immédiate du droit d'accès physique et d'accès aux systèmes devraient être mises en place, et les droits d'accès devraient être strictement appliqués.

79. Les entités critiques sont encouragées à n'accorder l'autorisation que sur la base du besoin d'en connaître ou du besoin d'accéder aux infrastructures, en ne donnant aux membres du personnel que le niveau minimal d'accès nécessaire pour accomplir leurs fonctions. Des stratégies de mise en œuvre telles que le contrôle d'accès fondé sur les rôles (RBAC) ([24]), l'authentification forte et la gestion de l'identité ([25]), la séparation des tâches ([26]), les restrictions fondées sur la durée et l'accès «juste à temps» ([27]) devraient être mises en place, de même que des audits et des examens réguliers.

80. En ce qui concerne la vérification des antécédents, afin de garantir un niveau élevé de sécurité du personnel, il importe de mettre en œuvre des procédures internes solides pour demander une vérification des antécédents conformément à l'article 14 de la directive et de désigner les catégories de personnes tenues de faire l'objet de telles vérifications. Des procédures de traitement des employés dont l'habilitation de sécurité est révoquée devraient également être mises en place.

81. Les entités critiques sont encouragées à définir leur politique de vérification des antécédents en précisant quelles fonctions sont sensibles, quelles fonctions requièrent un accès direct ou à distance aux locaux, aux informations ou aux systèmes de contrôle, et quels types de contrôles doivent être effectués pour chaque fonction sensible, tels que la vérification de l'identité, le contrôle des casiers judiciaires et la vérification des informations relatives à l'emploi et à l'éducation.

82. Le cas échéant, les mesures devraient être cohérentes avec les activités de vérification des antécédents prévues par le règlement d'exécution (UE) 2024/2690 de la Commission ([28]). Il convient également d'assurer la cohérence avec les mesures de sécurité en matière de ressources humaines prises par l'entité en question conformément à l'article 21, paragraphe 2, point i), de la directive SRI 2.

([24]) Il peut s'agir de définir des rôles spécifiques, par exemple «agent de sécurité physique», d'attribuer un ensemble prédéfini de droits d'accès et d'affecter le personnel aux rôles concernés.

([25]) Il peut s'agir d'une authentification multifactorielle et d'identifiants uniques.

([26]) Il peut s'agir de concevoir des contrôles d'accès afin de garantir qu'aucune personne ne dispose d'un accès suffisant pour réaliser, à elle seule, l'ensemble d'un processus critique à haut risque. Par exemple, la personne qui approuve une modification du système ne devrait pas être la même que celle qui applique cette modification.

([27]) Les membres du personnel ne devraient se voir accorder l'accès que temporairement, lorsqu'ils en ont activement besoin pour des tâches précises. Leur accès devrait ensuite être révoqué sans délai. Une politique limitant les droits d'accès en dehors des horaires de travail spécifiques devrait être mise en place, le cas échéant.

([28]) Voir point 10.2 de l'annexe.

83. En exigeant de son personnel qu'il dispose de qualifications et d'une formation adéquates, et en dispensant cette formation, l'entité critique pourra garantir une gestion appropriée de la sécurité de ses employés, sensibiliser le personnel à ses mesures de résilience et favoriser l'application des mesures en question. L'évaluation des risques d'entité critique, le type de services essentiels que fournit l'entité et les mesures prévues ou adoptées devraient déterminer le type et la portée de la formation nécessaire pour son personnel, afin de garantir que celui-ci soit non seulement familiarisé avec l'ensemble des mesures de résilience, mais aussi doté des compétences techniques et procédurales adéquates pour exécuter ses tâches de manière résiliente.

84. Les exigences en matière de formation et de qualification concernent, entre autres, l'évaluation des risques (par ex. pour le personnel chargé de la gestion/de la conformité vis-à-vis des risques), la continuité des activités et la gestion des crises (par ex. pour le personnel chargé de la continuité des activités), la sécurité physique (par ex. pour les agents de sécurité et les personnes ayant des droits d'accès), l'intervention et l'atténuation en cas d'incident (par ex. pour le personnel responsable des activités, les intervenants désignés en cas d'incident), le contrôle et la vérification des accès (ressources humaines, agents de sécurité et gestionnaires des fonctions critiques), ainsi que la sensibilisation générale aux mesures de résilience (pour l'ensemble du personnel).

85. Les exigences en matière de qualifications dépendent des particularités de l'entité critique en question et des services essentiels qu'elle fournit. L'objectif de ces exigences devrait être de garantir que le personnel a les compétences requises pour exécuter les tâches décrites dans l'évaluation des risques et le plan de résilience, ainsi que dans les protocoles de continuité des activités et d'intervention en cas d'incident intégrés dans le plan de résilience, dans le cadre des mesures de résilience adoptées par les entités critiques. Les exigences en matière de qualifications concernent les tâches opérationnelles et techniques, les tâches organisationnelles et de gestion, ou les tâches de sécurité et de vérification. Les qualifications requises devraient être définies dans les politiques internes de résilience et de ressources humaines de l'entité critique en question.

G. MESURES DE SENSIBILISATION [article 13, paragraphe 1, point f), de la directive]

86. Il est essentiel que chaque entité critique dispose d'un bon programme visant à sensibiliser son personnel aux mesures de résilience qu'elle a adoptées et à instaurer une culture de la sécurité; le personnel est un élément crucial de chaque étape du cycle de résilience, qu'il s'agisse de prévenir les incidents perturbateurs, d'atténuer les menaces internes ou d'y répondre en activant les procédures pertinentes, en signalant les incidents et en assurant la continuité des activités, ainsi qu'en garantissant la reprise des activités dans les mêmes conditions qu'avant l'incident. Si le personnel n'est pas bien informé, même les meilleures mesures techniques, organisationnelles et de sécurité pourraient échouer.

87. En fonction du niveau de sensibilité des informations et sur la base du besoin d'en connaître, la sensibilisation aux mesures de résilience garantit l'établissement optimal d'une culture de la résilience qui fait de cet aspect une valeur partagée par le personnel de l'entité critique et réduit le risque de menaces internes ou d'ingénierie sociale.

88. Il conviendrait d'adopter des mesures de sensibilisation conjointement aux mesures relatives aux pratiques de cyberhygiène de base et à la formation à la cybersécurité prévues par la directive SRI 2 ([29]).

89. La formation dispensée par une entité critique doit être reliée aux exigences de formation de cette entité critique mentionnées aux points 82 et 83 ci-dessus.. Les programmes de formation devraient couvrir les mesures de résilience prises par l'entité conformément à l'article 13, paragraphe 1, points a) à e), de la directive, couvrant ainsi l'ensemble du cycle de la résilience. Il convient pour cela de comprendre l'environnement des menaces, le rôle de l'entité critique dans le maintien des fonctions sociétales vitales et les graves conséquences de toute perturbation des services, de détecter et de signaler rapidement les activités suspectes, les vulnérabilités ou les incidents inhabituels, ainsi que de réagir aux incidents et de les atténuer. Le personnel exerçant des fonctions critiques devrait recevoir une formation spécifique à ces fonctions.

90. Les entités critiques sont également encouragées à dispenser une formation sur les approches tenant compte de la dimension de genre qui, associée au suivi des indicateurs pertinents, pourra renforcer la résilience, la responsabilité et la durabilité à long terme.

([29]) Article 21, paragraphe 2, point g), de la directive SRI 2.

91. Les supports d'information partagés avec le personnel devraient être directement liés à l'évaluation des risques de l'entité et aux mesures de résilience adoptées. Ces supports d'information devraient être clairs et faciles à assimiler, et expliquer le rôle critique de l'entité ainsi que l'incidence qu'auraient les perturbations sur la société et l'économie, la couverture «tous risques», les principes de sécurité fondamentaux tels que «si vous voyez quelque chose, signalez-le» et le principe du «moindre privilège» appliqué à l'accès aux informations sensibles.

92. Les supports d'information pourraient comprendre des supports visuels permettant de se reporter rapidement aux sections consacrées, par exemple, aux atteintes à la sécurité physique, à la perte de puissance/connectivité, à la découverte de colis suspects, aux diagrammes de notification des incidents et aux rappels concernant la continuité des activités extraits du plan de continuité des activités, des lignes directrices en matière de protection physique et des politiques de contrôle des accès. Pour maximiser la sensibilisation, ces supports devraient être fournis dans de multiples formats, numériques ([30]) et physiques ([31]), et être interactifs ([32]).

93. La réalisation d'exercices est cruciale pour valider le plan de résilience d'une entité critique et veiller à ce que son personnel puisse accomplir efficacement ses fonctions en cas d'incident réel. Dans le cadre d'une approche «tous risques», les entités pourraient organiser des exercices fondés sur la discussion, tels que des simulations sur table ([33]), et des exercices pratiques, tels que des simulations d'urgence ([34]).

94. Lorsqu'elles organisent de tels exercices, les entités critiques devraient se concentrer sur les résultats de leur évaluation des risques, tester l'ensemble du cycle de résilience et assurer une bonne coordination intersectorielle avec d'autres entités critiques, le cas échéant, afin de mettre à l'épreuve les dépendances intersectorielles. Elles devraient assurer la coopération avec les autorités publiques compétentes, telles que les services répressifs, les pompiers, les autres services d'urgence et, globalement, les premiers intervenants en cas d'incidents perturbateurs, et faire participer ces autorités publiques aux exercices.

([30]) Par exemple: intranet, modules obligatoires d'apprentissage en ligne avec des questionnaires, courtes vidéos, écrans de veille affichant des rappels essentiels en matière de sécurité.

([31]) Par exemple: affiches, dépliants, aide-mémoire.

([32]) Par exemple: foire aux questions.

([33]) Pour mettre à l'épreuve les procédures de coordination, de prise de décision et de communication lors d'un incident simulé (par ex. défaillance majeure de l'infrastructure, coupure de courant prolongée, violation de la sécurité interne).

([34]) Pour mettre à l'épreuve une procédure spécifique en situation d'urgence, telle que l'activation du générateur de secours, l'évacuation d'une zone critique ou l'isolement d'un tableau de commande compromis.