# Communication du Conseil de l'IBPT du 5 juillet 2022 concernant la plateforme SERIMA.be (analyse de risque en matière de sécurité des réseaux et des systèmes d'information)

**Institut belge des services postaux et des télécommunications**
Bâtiment Ellipse C | Boulevard du Roi Albert II 35 bte 1 | 1030 Bruxelles
**T** +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.ibpt.be**

# Table des matières

# 1. Objet

1. Le secteur des communications électroniques (en ce compris les infrastructures numériques) comprend des éléments essentiels pour le fonctionnement de la société et des services publics. La sécurisation de tous les éléments, aussi bien matériels qu'organisationnels, doit être une priorité de tous les acteurs de ce secteur. En atteignant un niveau de sécurité suffisant, non seulement un acteur du secteur protège ses propres activités mais, en plus, les services des autres acteurs du secteur en profitent, vu les interdépendances multiples entre les différents acteurs et services.

2. Dans ce contexte, l'article 107/2, § 1er, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la « LCE ») prévoit que chaque opérateur télécom doit :

   2.1. analyser les risques pour la sécurité de ses réseaux et services, l'IBPT pouvant fixer les modalités de cette analyse de risque ;

   2.2. prendre « *les mesures d'ordre technique et organisationnel adéquates et proportionnées, y compris le cas échéant le chiffrement, pour gérer ces risques de manière appropriée ainsi que pour prévenir et limiter l'impact des incidents de sécurité tant pour les utilisateurs que pour d'autres réseaux et services* ».

3. Pour ce qui concerne la deuxième obligation (l'obligation portant sur les mesures), l'article 20 de la loi NIS[1], qui s'applique aux opérateurs de services essentiels (OSE) entre autres du secteur des infrastructures numériques, comprend une disposition similaire. L'IBPT a été désigné comme autorité sectorielle et service d'inspection pour ce secteur dans le cadre de la loi NIS et a procédé à la désignation des OSE. Les OSE et les opérateurs télécoms sont désignés ci-après les « opérateurs ».

4. La présente communication a pour objectif d'informer le secteur du remplacement par l'IBPT de l'outil d'analyse de risques en matière de sécurité des réseaux et systèmes d'information (ci-après « la plateforme SERIMA.be »[2]). Cet outil est voué :

   - à faciliter l'échange d'informations entre les opérateurs et l'IBPT, notamment dans le cadre du contrôle du respect de l'article 107/2, §1er, al. 1er, de la LCE et de l'article 20, § 1er, de la loi NIS, et ;
   - à permettre aux opérateurs de s'auto-évaluer et d'accroître leur niveau de sécurité.

5. Dans un premier temps, l'IBPT demandera aux OSE et à certains opérateurs télécom (vu leur importance significative pour la société et l'économie belges) d'utiliser la plateforme SERIMA.be. Les autres opérateurs télécom peuvent faire usage de l'outil en adressant une demande à l'IBPT et moyennant le respect des conditions visées dans la présente communication. Dans un deuxième temps, après une analyse des interdépendances et sur base du retour d'expérience, l'IBPT examinera l'opportunité d'élargir le nombre d'utilisateurs de la plateforme.

---

[1] Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
[2] Abréviation de « Security Risk Management ».

6. Cette communication remplace la communication du 26/10/2020 à la suite du changement de l'outil d'analyse de risque.

## 2. Cadre juridique

7. En vertu de l'article 6, 4°, de la LCE, l'IBPT « promeut les intérêts des citoyens » « en préservant la sécurité des réseaux et services ».

8. L'article 107/2, §1er, de la loi télécom prévoit que l'IBPT peut fixer les modalités de l'analyse de risque en matière de sécurité des réseaux et des services que les opérateurs doivent effectuer.

9. L'article 107/4, §1er, de la LCE précise que, dans le cadre de ce contrôle, l'IBPT a le pouvoir de donner des instructions contraignantes, y compris concernant les dates limites de mise en oeuvre, aux opérateurs télécoms.

10. L'IBPT peut également, conformément à l'article 107/4, § 2 LCE, solliciter de ces mêmes opérateurs télécoms toutes les informations nécessaires pour évaluer la sécurité ou l'intégrité, ou les deux, de leurs services et réseaux, y compris les documents relatifs à leur politique de sécurité (alinéa 1er), ainsi que soumettre ces opérateurs télécoms à un contrôle de sécurité effectué par un organisme qualifié indépendant ou l'Institut lui-même (alinéa 2).

11. Par ailleurs, l'IBPT a été désigné comme service d'inspection pour le secteur des infrastructures numériques dans le cadre de la loi NIS, qui prévoit entre autres que :

- « Les services d'inspection peuvent à tout moment réaliser des contrôles du respect par l'opérateur de services essentiels des mesures de sécurité et des règles de notification des incidents. » (article 42, § 1er) ;
- Le service d'inspection peut formuler une demande d'informations ou de preuves (article 42, § 3) ;
- « L'opérateur de services essentiels apporte son entière collaboration aux membres du service d'inspection dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes. » (article 46, § 1er).

12. Ensuite l'article 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (ci-après la loi « infrastructures critiques ») prévoit que « *Pour le secteur des communications électroniques et des infrastructures numériques, l'Institut belge des services postaux et des télécommunications est désigné en tant que service d'inspection chargé de contrôler l'application des dispositions de la présente loi et de ses arrêtés d'exécution.* »

13. Finalement, conformément à l'article 14, §1er, 3°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (loi statut), l'IBPT est chargé de contrôler le respect entre autres des dispositions :

13.1. de la LCE ;

13.2. de la loi « infrastructures critiques », pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques, et ;

13.3. de la loi NIS pour ce qui concerne le secteur des infrastructures numériques.

## 3. Mesures de sécurité et analyse de risques

14. Conformément à l'article 107/2, § 1er, les opérateurs doivent analyser les risques pour la sécurité de leurs réseaux et services. Une analyse de risque conforme à cette disposition suppose qu'elle soit mise à jour lorsque c'est nécessaire.

15. Une analyse de risques se compose de trois étapes principales [3] :

- L'identification des risques ;
- L'évaluation des risques ;
- La gestion des risques.

16. Afin d'être utilisable, une analyse de risque doit répondre aux conditions suivantes :

- être exécutée pour tous les actifs indispensables au bon fonctionnement des réseaux[4] ;
- confronter les actifs avec des menaces ;
- pour chaque couple d'actif-menace, identifier les vulnérabilités ;
- sur la base de l'identification des vulnérabilités, adopter des mesures de sécurité visant à supprimer, ou à défaut de réduire, l'impact et/ou la probabilité de l'exploitation d'une vulnérabilité et, par conséquence, supprimer, ou à défaut réduire, le risque.

[3] Ceci découle des normes en matière de sécurité des réseaux : ISO/IEC 27005, NIST Special Publication 800-37, BS 7799-3 BSI.
[4] Par définition, les actifs d'une société représentent toutes les ressources matérielles, humaines, administratives ou organisationnelles rentrant en compte dans la fourniture de ses services ou produits.

# 4. La plateforme SERIMA.be

## 4.1. Description générale

17. La plateforme SERIMA.be permet d'effectuer une analyse complète des risques selon la méthodologie prévue par la norme ISO/IEC 27005 relative aux technologies de l'information, techniques de sécurité et gestion des risques liés à la sécurité de l'information, qui constitue une norme pertinente pour l'application de différentes réglementations incluant des aspects de gestion de risques, comme l'article 107/2, § 1er, de la LCE, l'article 20 de la loi NIS et le RGPD[5]. L'IBPT n'examinera bien entendu que le respect de la LCE et de la loi NIS (pour le secteur des infrastructures numériques).

18. La plateforme SERIMA.be est basée sur l'outil MONARC[6] mis en œuvre par SecurityMadeIn.LU[7]. Il s'agit d'un outil « Open Source » disponible sur https://monarc.lu.

19. Compte tenu des contextes multiples d'application de la norme ISO/IEC 27005, la plateforme SERIMA.be a été conçue pour permettre aux entreprises de faire l'analyse en tenant compte de différentes réglementations.

20. En outre, la plateforme SERIMA.be peut être utilisée par tout opérateur ayant accès à cette dernière, comme système de gestion des risques pour d'autres référentiels[8], tels que les référentiels propres à l'entreprise.

21. La plateforme SERIMA.be a vocation à évoluer, selon le retour d'expérience (« feedback ») de ses utilisateurs, notamment en ce qui concerne la mise à jour des librairies, la correction des fonctionnalités existantes ainsi que l'ajout d'éventuelles fonctionnalités.

22. La plateforme SERIMA.be permet à tout opérateur télécom de réaliser une analyse de risque appropriée et d'évaluer les mesures de sécurité déjà en place en son sein, selon la méthodologie décrite dans les « Technical guidelines of security measures »[9] de l'ENISA. Les éléments pertinents pour l'IBPT, dans le cadre de ses missions légales, peuvent ensuite être sélectionnés par l'entreprise et transmis à l'IBPT.

## 4.2. Objectifs visés

23. La plateforme SERIMA.be a pour objectif premier de faciliter l'échange d'informations entre les opérateurs et l'IBPT dans le cadre du contrôle du respect de la LCE et la loi NIS.

24. Plus précisément, la transmission des informations par le biais de la plateforme SERIMA.be permettra à l'IBPT :

---

[5] Règlement nº 2016/679, dit règlement général sur la protection des données.
[6] MÉTHODE OPTIMISÉE D'ANALYSE DES RISQUES, https://monarc.lu
[7] https://securitymadein.lu/
[8] ISO27001, GDPR ou un référentiel défini par l'entreprise.
[9] https://resilience.enisa.europa.eu/article-13

- de disposer d'un aperçu plus clair et précis quant au niveau de sécurité de chaque opérateur en matière de sécurité des réseaux et services ;
- d'observer l'évolution de la situation d'un opérateur d'année en année ;
- de comparer de manière aisée et automatisée les données entre opérateurs, grâce au recours à une même méthodologie et à la standardisation du format des données.

25. En outre, l'observation sous une forme agrégée des données transmises à la plateforme SERIMA.be permettra à l'IBPT d'en tirer les enseignements utiles, tels que par exemple l'identification des risques communs à la plupart ou à l'ensemble des opérateurs, les bonnes pratiques pour ce qui concerne les mesures de sécurité, etc. Ces observations permettront notamment de contribuer à fixer les niveaux de priorité de ses domaines d'intervention.

26. Par ailleurs, l'IBPT pourra faire bénéficier le secteur de ces enseignements :

- Par la transmission à chaque opérateur utilisant la plateforme, après examen des données transmises par le biais de cette plateforme, d'un rapport individuel de leur gestion des risques afin de les soutenir dans leur gestion de la sécurité ;
- Par la publication d'un rapport général d'aide à la gestion des risques à destination de tous les acteurs du secteur ;
- Par le maintien d'une communauté d'utilisateurs autour de la plateforme. Cette communauté permettra l'échange d'information relatif à l'évaluation des risques et des mesures de sécurité.

## 4.3. Informations pratiques

### 4.3.1. Accès à la plateforme

27. Les accès doivent être demandés par courriel à sec_netsec@bipt.be. Le service sécurité des réseaux validera la demande auprès du point de contact visé à l'article 9, § 1er, 5° de la loi du 13 juin 2005 relatives aux communications électroniques pour les opérateurs télécom ou auprès du point de contact visé à l'article 23, § 1er, de la loi NIS. Une adresse électronique doit être fournie avec la demande ainsi qu'un numéro de téléphone. Le service sécurité des réseaux fournira alors la documentation de la plateforme ainsi que les données nécessaires pour s'y connecter.

28. L'opérateur a également la possibilité d'installer l'outil d'analyse de risque directement dans son propre environnement informatique. L'outil est disponible sur le site de SecurityMadeIn.LU[10]. Tous les coûts liés à sa propre instance de l'outil d'analyse de risque sont à ses propres frais. Il est important de rappeler qu'il s'agit d'un outil « Open Source » pour lequel aucune licence n'est nécessaire. Dans ce cas, l'opérateur doit utiliser les librairies proposées par l'IBPT pour les analyses qui seront soumises à l'IBPT. Les accès aux librairies doivent être demandés par courriel à sec_netsec@bipt.be.

29. La documentation générale sur l'outil d'analyse de risque MONARC est disponible sur https://www.monarc.lu/documentation/.

[10] https://www.monarc.lu/download/

### 4.3.2. Informations à prendre en compte

30. Pour que l'analyse de risque via SERIMA.be soit efficace, il convient de répondre à un certain nombre d'éléments.

31. Les services suivants sont par défaut à considérer dans l'analyse :

- Fibres (noires) ou réseau de fibres : exploitation, mises à disposition et/ou maintenance de ces fibres ;
- Données : mobile, fixe, transit, interconnexions, VPN ;
- Voix : mobile, fixe, interconnexions ;
- SMS.

32. Les services suivants peuvent être considérés dans l'analyse : courriel, messagerie instantanée.

33. Tant les services de communications électroniques de détail (« retail ») que les services aux entreprises (« business ») et à d'autres opérateurs (« wholesale ») sont à considérer lors de l'utilisation de la plateforme, puisque chacun de ces types de services est susceptible d'avoir un impact significatif sur le bon fonctionnement de la société et de l'économie.

34. Pour qu'une soumission soit valide, les informations marquées « obligatoires » dans la plateforme SERIMA.be doivent avoir été remplies avec exactitude et probité. Il s'agit :

- des données générales du projet ;
- des données définissant le contexte de l'analyse de risque ;
- des données liées à l'analyse de risque pour l'ensemble des service offerts, des actifs qui les supportent, à mettre en relation avec au minimum les menaces reprises comme « obligatoires » ;
- des données décrivant les mesures déjà en place[11] et l'évaluation du niveau de sécurité.

35. Pour les années 2022 et suivantes, les opérateurs sont invités à soumettre ce formulaire à l'IBPT au minimum une fois par an, entre le 1 décembre et le 31 décembre au plus tard, par le biais de la plateforme SERIMA.be mise à leur disposition ou en fournissant à l'IBPT un export de leur propre instance de Monarc.

36. Dans le cas où l'IBPT rejette de manière motivée la soumission du formulaire au motif que cette dernière n'est pas valide, l'opérateur a la possibilité de soumettre un formulaire corrigé dans le délai fixé par l'IBPT.

[11] Il est suffisant que l'outil reprenne une forme agrégée des mesures mises en place ou la référence vers la documentation pertinente.

### 4.3.3. Formations

37. Des formations à l'utilisation de la plateforme SERIMA.be seront proposées périodiquement par l'intermédiaire de l'IBPT ou par SecurityMadeIn.LU[12].

[12] https://www.monarc.lu/trainings/

## 5. Conclusions

38. Dans un premier temps, l'IBPT demandera aux OSE et à certains opérateurs télécom (vu leur importance significative pour la société et l'économie belges) d'utiliser la plateforme SERIMA.be. Les autres opérateurs télécom peuvent faire usage de l'outil en adressant une demande à l'IBPT et moyennant le respect des conditions visées dans la présente communication. Dans un deuxième temps et sur base d'un retour d'expérience, l'IBPT examinera l'opportunité d'élargir le nombre d'utilisateurs de la plateforme.

39. Après examen des données transmises par le biais de la plateforme SERIMA.be, l'IBPT transmettra à chaque opérateur un rapport générique et un rapport individuel de leur gestion des risques afin de les soutenir dans leur gestion de la sécurité.

Axel Desmedt
Membre du Conseil

Bernardo Herman
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Michel Van Bellinghen
Président du Conseil