

FR

Plan gouvernemental de gestion de crise cybernétique et numérique

VERSION PUBLIQUE 12/09/2025

*Approuvé et rendu exécutoire
par le Conseil de Gouvernement
le 12 septembre 2025*



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sommaire

1.	Introduction	3
2.	Cadre national et européen	4
3.	Concepts clés	5
3.1.	Classification nationale des incidents de cybersécurité	5
3.2.	Classification des cybermenaces	5
4.	Modes de coopération	6
4.1.	Mode « Permanent »	6
4.2.	Mode « Alerte / CERC »	6
4.3.	Mode « Crise »	6
5.	Organes de gestion de crise	7
5.1.	Cellule d'Évaluation du Risque Cyber (CERC)	7
5.2.	Cellule de Crise (CC)	7
5.3.	Cellule Opérationnelle Cyber (PCO-C)	8
5.4.	Cellule Communication et Information (CCI)	8
6.	Mesures à prendre	9
6.1.	Évaluation	9
6.2.	Veille renforcée	9
6.3.	Mise à niveau et protection des systèmes	9
6.4.	Rétablissement des services	9
7.	Collaboration et assistance internationale	10
8.	Information du public	10

1. Introduction

Le présent plan gouvernemental de gestion de crise cybernétique et numérique définit le cadre directeur de préparation, de coordination et de réponse de l'État luxembourgeois face aux crises cybernétiques ou numériques susceptibles de porter atteinte aux intérêts vitaux ou aux besoins essentiels de tout ou partie du pays ou de sa population, notamment en cas de défaillance technique majeure ou d'attaque d'envergure contre les systèmes d'information des secteurs public et/ou privé.

Ce plan s'inscrit dans la continuité du Plan d'Intervention d'Urgence Cyber (PIU Cyber), afin d'assurer la pérennité de la conformité et de la résilience de l'État, les mutations de la menace et les exigences des cadres réglementaires nationaux et communautaires.

Le plan a pour objectifs principaux :

- de renforcer la préparation, la prévention et la protection face aux risques cybernétiques et numériques ;
- de définir les principes de gouvernance et les organes de gestion de crise nécessaires à une coordination nationale efficace ;
- de fixer les modalités générales de réponse et de gestion des situations de crise, ainsi que les rôles respectifs des acteurs impliqués ;
- de déterminer le cadre de diffusion de l'alerte par les autorités et de l'information à destination du public.

Il s'applique aux situations dans lesquelles la gravité réelle ou potentielle d'un événement exige des décisions urgentes et une coordination au niveau national et, le cas échéant, une articulation avec les mécanismes européens et internationaux de gestion de crise.

Une situation d'urgence cybernétique ou numérique désigne un événement, résultant d'un incident ou d'une cybermenace, susceptible d'entraîner un dysfonctionnement majeur ou l'indisponibilité des systèmes de communication et de traitement de l'information, et qui porte ou est susceptible de porter atteinte aux intérêts vitaux ou aux besoins essentiels de tout ou partie du pays ou de la population du Grand-Duché de Luxembourg.

L'élaboration et la coordination du présent plan relèvent du Haut-Commissariat à la protection nationale (HCPN). Son exécution s'inscrit dans le cadre de la responsabilité gouvernementale et mobilise, en fonction de la nature et de la gravité de la situation, l'ensemble des ministères, administrations et services de l'État concernés, qui coopèrent à la réalisation des objectifs fixés, dans le respect du mandat de chaque partie prenante.

2. Cadre national et européen

Le plan s'inscrit dans le dispositif national de gestion de crise coordonné par le Haut-Commissariat à la protection nationale (HCPN) et s'aligne sur les cadres européens en matière de cybersécurité et de gestion de crise, notamment :

- › la 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 (directive NIS 2) ;
- › la recommandation du Conseil de l'Union européenne du 6 juin 2025 relative au Cyber Blueprint pour la gestion des crises de cybersécurité ;
- › les mécanismes européens de coopération et de coordination en matière de gestion de crise, en particulier le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (IPCR) et le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe).

Ce positionnement assure l'alignement entre la réponse luxembourgeoise et les approches européennes, en particulier lorsqu'une crise cybernétique présente des implications transfrontalières.

3. Concepts clés

3.1. Classification nationale des incidents de cybersécurité

Afin de permettre une réponse rapide, proportionnée et coordonnée, le cadre national distingue notamment :

- › **Incident de cybersécurité transfrontière majeur** : incident provoquant des perturbations excédant les capacités de réaction du Luxembourg ou qui a un impact important sur au moins un autre État membre ou pays tiers ;
- › **Incident de cybersécurité national majeur** : incident provoquant des perturbations portant préjudice aux intérêts vitaux ou aux besoins essentiels de tout ou partie du pays ou de la population, requérant des décisions urgentes et une coordination au niveau national ;
- › **Incident important** : incident qui a
 - causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l’entité concernée ;
 - affecté ou est susceptible d’affecter d’autres personnes physiques ou morales causant des dommages matériels, corporels ou moraux considérables.
- › **Incident** : événement compromettant la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles.

Cette classification permet d’évaluer l’envergure de l’incident et d’adapter le mode de coopération et le niveau de mobilisation des acteurs concernés.

3.2. Classification des cybermenaces

Le plan distingue également plusieurs niveaux de cybermenaces, en fonction de leur potentiel d’impact, de leur portée et de la nature des cibles visées, afin d’anticiper les mesures de vigilance et de coopération appropriées.

4. Modes de coopération

Le dispositif repose sur trois modes de coopération complémentaires.

4.1. Mode « Permanent »

En dehors de toute crise, le plan fonctionne en mode permanent. Celui-ci est dédié à la préparation et comprend notamment :

- › la surveillance continue de l'évolution des cybermenaces et des risques systémiques ;
- › l'adaptation et la mise à jour des plans et procédures ;
- › l'organisation régulière d'exercices et de tests.

4.2. Mode « Alerte / CERC »

Lorsqu'un événement présente un risque de préjudice significatif sans toutefois constituer une crise avérée, la coordination s'opère dans le cadre du mode « Alerte / CERC ». Ce mode assure une vigilance renforcée, facilite un partage rapide et ciblé des informations entre les acteurs concernés et permet la mise en œuvre précoce de mesures d'atténuation, afin de prévenir toute escalade vers une situation de crise.

4.3. Mode « Crise »

Lorsqu'un événement cybernétique ou numérique porte atteinte aux intérêts vitaux ou aux besoins essentiels, le mode « Crise » est activé pour assurer une gestion nationale concertée et efficiente.

Ce mode permet d'activer les dispositifs de réponse prévus, de structurer les échanges d'informations nécessaires à la compréhension et au suivi de l'événement, et d'intégrer l'action cyber avec les autres cadres de gestion de crise, qu'ils soient nationaux ou sectoriels.

5. Organes de gestion de crise

5.1. Cellule d'Évaluation du Risque Cyber (CERC)

La Cellule d'Évaluation du Risque Cyber (CERC) est investie de l'analyse, de l'évaluation et du suivi des incidents de cybersécurité et des cybermenaces. Elle assure une veille renforcée, évalue la gravité et l'impact potentiel des événements et formule, le cas échéant, des recommandations, notamment en vue d'un passage vers le mode « Crise ».

5.2. Cellule de Crise (CC)

En mode « Crise », la gestion s'appuie sur une structure de gouvernance adaptée à la nature et à l'ampleur de l'événement.

La Cellule de Crise (CC) est activée par le Premier ministre, en cas d'imminence ou de survenance d'une crise. Elle initie, coordonne et veille à l'exécution de toutes les mesures visant à maîtriser la situation et à en atténuer les effets, tout en favorisant un retour à la normale. Elle élabore les décisions qui s'imposent et les soumet à l'approbation du Gouvernement. En cas d'intervention opérationnelle, sa mission s'étend à la coordination et au contrôle de l'exécution.

En situation d'urgence, la Cellule de Crise est composée au minimum des personnes suivantes :

1. Le Haut-Commissaire à la protection nationale.
2. Le secrétaire général du Gouvernement.
3. Le Directeur général de la Police grand-ducale.
4. Le Chef d'État-major de l'Armée.
5. Le Directeur du Service de renseignement de l'État.
6. Le Directeur du Centre des technologies de l'information de l'État.
7. Le Directeur du Service des médias, de la connectivité et de la politique numérique.
8. Le Directeur de l'Institut luxembourgeois de régulation.
9. Un représentant du ministère de l'Économie.
10. Un représentant du ministère de la Digitalisation.

La Cellule de Crise demeure active durant toute la période de crise et jusqu'au rétablissement de la situation.

La CC peut être élargie, selon les circonstances et les sujets devant être discutés par des représentants d'autres entités publiques, notamment la Commission de

Surveillance du Secteur Financier (CSSF), l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS), la Direction de l'aviation civile (DAC), les ministères impactés en cas de crise cyber intersectorielle, les communes impactées ainsi que par des représentants des opérateurs/propriétaires d'infrastructures critiques.

En cas d'empêchement, les membres de la CC sont tenus de se faire remplacer.

La Cellule de Crise suit l'évolution de la situation sur base des informations élaborées à son intention par la Cellule Opérationnelle Cyber (PCO-C).

5.3. Cellule Opérationnelle Cyber (PCO-C)

La Cellule de Crise peut déléguer à la Cellule Opérationnelle Cyber l'exécution, la mise en œuvre et le contrôle des mesures et activités décidées. La Cellule Opérationnelle Cyber assure le rôle de la Cellule d'Évaluation du Risque Cyber (CERC), tout en assurant la coordination et la mise en œuvre opérationnelle des mesures arrêtées et le lien entre les niveaux stratégique et technique.

5.4. Cellule Communication et Information (CCI)

La Cellule Communication et Information (CCI) est chargée de la communication et de l'information à destination des médias et des citoyens. Elle est responsable de la communication publique et institutionnelle et assure une information claire, cohérente et coordonnée à l'attention des citoyens, des médias et des parties prenantes.

La coordination horizontale de la communication externe relève du Service de la communication de crise du HCPN, notamment afin de prévenir la mésinformation et de garantir la cohérence des messages diffusés.

En principe, la Cellule Communication et Information (CCI) est convoquée en parallèle de la Cellule de Crise et est chargée de la communication et de l'information à destination des médias et de la population. Sa composition reflète, dans la mesure du possible, celle de la CC. La CCI informe régulièrement le grand public sur l'incident, son évolution, ainsi que sur les mesures prises par les autorités nationales.

Les informations officielles sont diffusées par les canaux institutionnels du Gouvernement, notamment le portail www.infocrise.lu. Selon la nature, la gravité et l'urgence de la situation, le Gouvernement peut recourir au système national d'alerte à la population LU Alert, permettant une diffusion rapide et ciblée d'informations essentielles. Les alertes en cours sont communiquées via le site www.lu-alert.lu, **l'application mobile « LU-Alert »**, et, si nécessaire, par SMS géolocalisés ou messages par diffusion cellulaire (Cell Broadcast).

6. Mesures à prendre

Le plan met à la disposition des responsables en charge de sa mise en œuvre un ensemble de mesures permettant de réagir de manière appropriée, proportionnée et flexible aux événements cybernétiques ou numériques, afin de protéger les citoyens, les secteurs concernés, leurs intérêts vitaux ainsi que les intérêts vitaux nationaux.

6.1. Évaluation

L'évaluation constitue la première étape du cycle de gestion de crise. Elle vise à apprécier le degré d'urgence de l'événement, son ampleur ainsi que son impact réel ou potentiel sur les intérêts vitaux ou les besoins essentiels de tout ou partie du pays ou de sa population.

6.2. Veille renforcée

La veille renforcée regroupe les actions mises en œuvre lorsqu'une situation présente un risque accru, notamment l'analyse des informations disponibles ainsi que l'évaluation continue de l'évolution de la situation.

6.3. Mise à niveau et protection des systèmes

Cette mesure vise à limiter les risques d'exploitation de vulnérabilités techniques et peut conduire à la mise en œuvre de mesures de protection ou de limitation appropriées, sur recommandation du PCO-C et sur décision de la CC.

6.4. Rétablissement des services

Le rétablissement des services permet une reprise progressive des activités affectées, selon des priorités définies, jusqu'au retour à une situation normale et stable.

7. Collaboration et assistance internationale

Toute crise cybernétique étant susceptible de présenter une dimension internationale, une collaboration avec les partenaires étrangers est assurée. Une assistance internationale peut être sollicitée, notamment dans le cadre de la coopération entre équipes de réponse aux incidents et au sein des organisations internationales dont le Grand-Duché de Luxembourg est membre.

8. Information du public

L'information au public constitue un élément central de la gestion de crise. Le Gouvernement informe de manière régulière et coordonnée sur l'évolution de la situation, les impacts potentiels et les consignes à suivre.

Les informations officielles sont diffusées via les canaux institutionnels du Gouvernement, notamment le portail www.infocrise.lu. En fonction de la nature, de la gravité et de l'urgence de la situation, le Gouvernement peut recourir au système national d'alerte à la population LU-Alert, permettant la diffusion rapide et ciblée d'informations essentielles.

En complément, tout autre canal de diffusion jugé pertinent peut être utilisé afin d'assurer une transmission large, rapide et accessible des messages au plus grand nombre de citoyens.