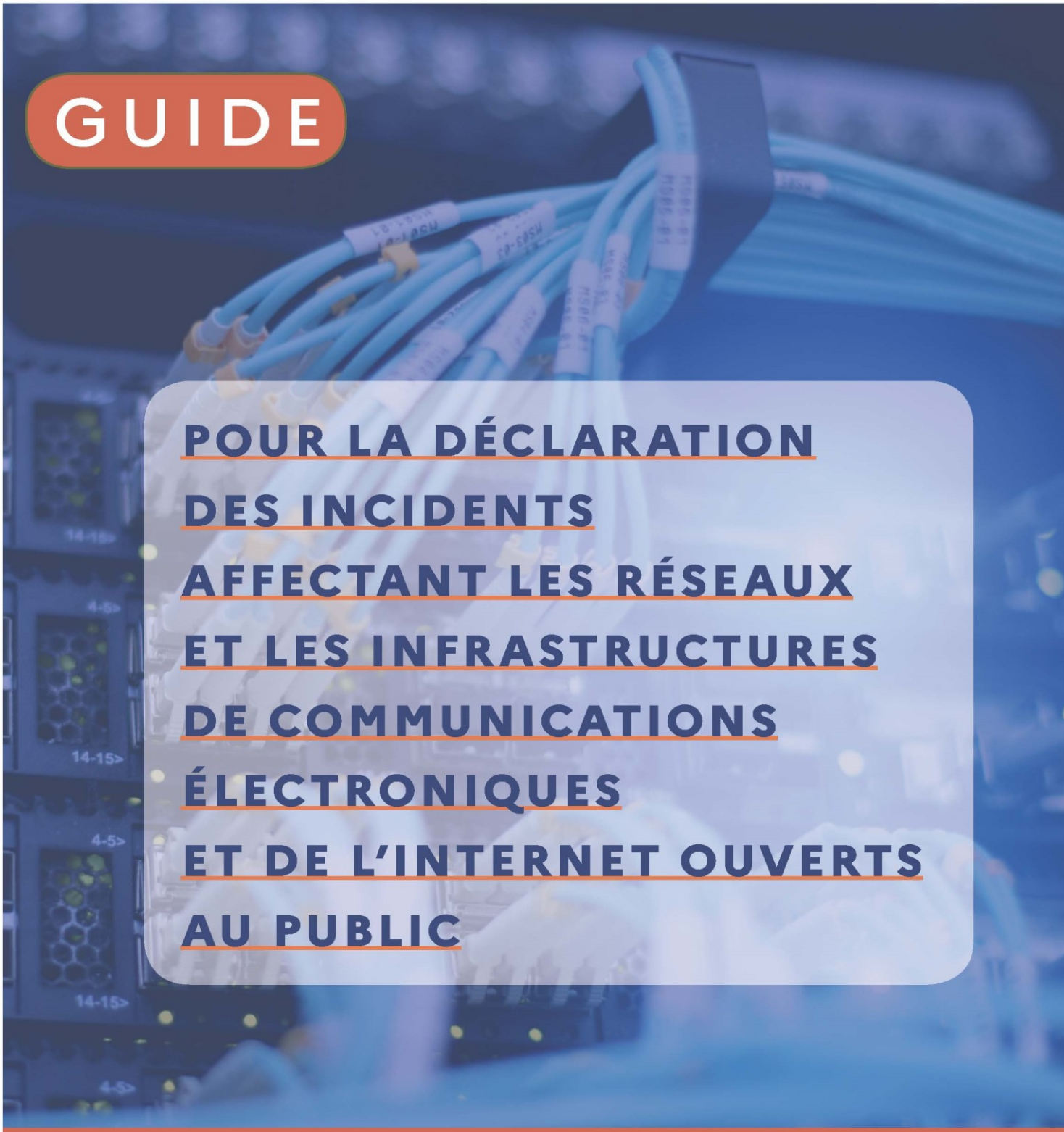
GOUVERNEMENT

Liberté
Égalité
Fraternité



GUIDE

POUR LA DÉCLARATION DES INCIDENTS AFFECTANT LES RÉSEAUX ET LES INFRASTRUCTURES DE COMMUNICATIONS ÉLECTRONIQUES ET DE L'INTERNET OUVERTS AU PUBLIC

SERVICE DU HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

COMMISSARIAT AUX COMMUNICATIONS ÉLECTRONIQUE DE DÉFENSE

Le présent guide constitue, pour les opérateurs relevant du Code des postes et des communications électroniques, la déclinaison pratique de l'obligation réglementaire instaurée par l'article D. 98-5 du Code des postes et des communications électroniques. Il tient compte des spécificités instaurées par l'article 34 de la loi n°2018-607 de programmation militaire 2019-2025[1] s'agissant des incidents de cyber-sécurité

Historique des versions

Ce document regroupe un ensemble de préconisations ayant pour objectif de préciser la manière dont les opérateurs de communications électroniques doivent satisfaire à leurs obligations légales en matière de déclaration d'incidents. Ce guide est régulièrement mis à jour pour tenir compte de l'expérience acquise sur des incidents réels, les évolutions réglementaires, et les retours des opérateurs.

Ce guide résulte des travaux du groupe de travail CICRESCE « Signalisation d'incidents » initié en 2012 et piloté par le CCED et l'ANSSI. Ce groupe réunissait des représentants des principaux opérateurs de réseaux de communications électroniques ouverts au public (Orange, SFR, Bouygues Télécom et Free) ainsi que des représentants de l'ARCEP et de la DGSCGC.

L'application de ce guide a ensuite été étendue à de nouveaux opérateurs jugés importants parmi les opérateurs de Datacenter, les hébergeurs Web, les fournisseurs de services aux entreprises et les plateformes de service.

La version 4 du guide est issue des travaux du CCED en 2022 pour définir un plan de résilience du dispositif des communications d'urgence. L'application de ce guide est étendue à tous les opérateurs de communications électroniques en métropole et en outre-mer. Les autres modifications concernent les seuils d'alerte qui ont été revus et l'introduction de la notion de « services essentiels » dont l'importance pour le fonctionnement des réseaux et des appels d'urgence nécessite un suivi particulier de la part des opérateurs.

Version du guide	Date de création	État
Version 3.0	27/05/2020	Abrogé
Version 4.0	22/03/2022	Abrogé
Version 4.1	20/04/2022	En vigueur
Version 4.2	29/07/2022	En vigueur

Tableau 1: historique des versions de ce guide

TABLE DES MATIÈRES

1. À QUOI SERT CE GUIDE ?

Comme le dispose l'article D.98-5 du code des postes et communications électroniques[1], les opérateurs de communications électroniques informent le ministre de l'Intérieur de tout incident de sécurité ayant un impact significatif sur le fonctionnement des réseaux ou des services.

Ce guide vise à préciser comment les opérateurs peuvent s'acquitter de cette obligation légale.

1. Caractériser la notion d'« **incident de sécurité ayant un impact significatif sur le fonctionnement des réseaux ou des services** »
2. Définir les **modalités pratiques de déclaration des incidents** en spécifiant :
    - les autorités à informer ;
    - les informations à fournir aux autorités ;
3. Servir de support de communication pour faire connaître cette procédure :
    - aux personnels des opérateurs concernés par le traitement des incidents ;
    - aux organisations de l'administration (DGSCGC/COGIC, ANSSI/COSSI, MEF/HFDS, MEFR/DGE/CCED) ayant à connaître de la survenance d'un incident chez un opérateur.

2. QUI SONT LES OPÉRATEURS CONCERNÉS ?

Sont concernés par la déclaration des incidents, au sens de la réglementation l'article D.98-5 du CPCE : **tous les opérateurs de réseaux de communications électroniques fixes ou mobiles exploitant un réseau ouvert au public et offrant tout ou partie des services de téléphonie ou d'accès à l'Internet**.

[1] Se référer à l'Annexe A pour le texte du décret

3. QUELS INCIDENTS DOIVENT ÊTRE DÉCLARÉS ?

Les opérateurs informent le ministre de l'intérieur de tout incident de sécurité ayant un impact significatif sur le fonctionnement de ses réseaux ou de ses services.

Nous définissons dans ce guide

Seuils caractérisant un incident significatif : Le *Tableau 2,* page suivante vise à préciser la notion d'impact significatif d'un incident. Il précise, pour les principaux services fournis par les opérateurs, les seuils établissant une frontière entre un incident significatif et un incident qui ne nécessite pas d'informer l'État. Selon les services, ces seuils portent sur :

a) Le nombre d'utilisateurs touchés par l'incident
b) La durée de l'incident ;
c) L'étendue géographique de la zone touchée par l'incident;
d) La mesure dans laquelle le fonctionnement du réseau ou du service est affecté ;
e) L'ampleur de l'impact sur les activités économiques et sociétales.

Les incidents d'intégrité : On entend par « incident d'intégrité » un incident résultant d'un dysfonctionnement technique des réseaux et infrastructures ayant un impact significatif sur le fonctionnement des services offerts par un opérateur.

Dès lors qu'un incident d'intégrité est significatif, l'opérateur prévient le ministère de l'intérieur.

Les incidents de sécurité : On entend par « incident de sécurité » la détection ou la suspicion d'une attaque sur les systèmes d'information des opérateurs, L'opérateur prévient le ministère de l'intérieur ainsi que l'autorité nationale de sécurité des systèmes d'information.

Dès lors qu'un incident de sécurité est significatif, l'opérateur prévient le ministère de l'intérieur, ainsi que l'autorité nationale de sécurité des systèmes d'information.

Tableau 2 - Seuils d'alerte aux autorités

Service de communication	Seuil pour alerter les autorités
Services de communications ouverts au public	
Téléphonie fixe ou mobile	Incident entrainant l'indisponibilité totale d'un service, concernant: • au moins 50 000 abonnés ou au moins 50 sites radios (sur une zone géographique limitée), • sur une durée de 2 heures
Accès Internet fixe ou mobile	
Services d'urgence	
Acheminement des appels d'urgence	Incident concernant les numéros d'urgence 15, 17 ou 18 et 112 (dont eCall) : • Taux d'efficacité des appels inférieur à 50% • Sur une durée de 1 heure
Services de localisation des appels d'urgences	Impossibilité de fournir l'un des services de localisation sur une durée dépassant 1 heure
Raccordement des PSAP[2] (pour les opérateurs de terminaison)	Indisponibilité totale du raccordement d'un PSAP sur une durée de 2 heures
Services essentiels	
Interconnexion entre opérateurs • Interconnexion voix • Interconnexion internationale • Interconnexion IP ou Internet	Baisse du taux d'efficacité du réseau d'au moins 40% sur l'interconnexion vers l'un des 4 principaux opérateurs[3] sur une durée dépassant 2 heures En cas de perte *totale* de l'interconnexion vers l'un de ces 4 opérateurs, le délai est ramené à 1 heure.
Service aux entreprises	
• Téléphonie fixe ou mobile. • Données fixe ou mobile	Indisponibilité totale d'un service sur : • une durée dépassant 2 heures • au moins 2000 établissements d'entreprise[4] impactés (quel que soit la taille de l'entreprise)
• Hébergement Web • Hébergement de données	

[2] Ce critère concerne un opérateur de terminaison, qui gère la connexion du réseau avec un centre de traitement des appels d'urgence

[3] Les 4 opérateurs principaux sont : Bouygues Télécom, Free, Orange et SFR

[4] La notion « d'établissement d'entreprise » désigne soit une entreprise avec un établissement unique, soit un site d'une entreprise quand celle-ci dispose de plusieurs établissements

4. QUELLES INFORMATIONS FOURNIR AUX AUTORITÉS ?

Lorsqu'un opérateur détecte un incident significatif sur son réseau celui-ci doit informer les autorités (indiquées au chapitre 6, *Où envoyer une déclaration ?)* en fournissant autant d'éléments que disponibles pour faciliter la compréhension de l'incident et son impact. Ainsi l'opérateur indiquera :

- une référence d'incident. Cette référence est créée par l'opérateur lors de la déclaration initiale et sera réutilisée pour toute déclaration de mise à jour et la déclaration de clôture ;
- un contact que les autorités pourront joindre pour s'informer sur l'incident en cours;
- un descriptif de l'incident, rédigé d'une manière claire et non technique, expliquant la nature et l'origine de l'incident;
- une évaluation de l'impact de l'incident en indiquant :
    - La nature du réseau concerné (mobile, fixe, Internet…) ;
    - Une estimation du nombre d'abonnés concernés ;
    - La localisation et l'étendue géographique de la zone concernée
    - dans le cas d'un incident sur un réseau mobile : le nombre de sites radios concernés

  Une attention particulière sera apportée pour préciser l'impact de l'incident sur les communications d'urgence
- une description des mesures prises pour assurer la continuité du service;
- une description des mesures prises pour retrouver un fonctionnement nominal ;
- une évaluation de l'évolution prévisible de l'incident : *par exemple, une estimation du temps nécessaire pour retrouver un service normal* ;
- l'opérateur doit contribuer, en concertation avec les autorités administratives, à la définition de mesures de contournement, de mesure conservatoire à prendre par l'administration, de consignes à donner aux usagers.

L'opérateur trouvera en Annexe B, le *Formulaire de déclaration d'incident* devant être utilisé pour émettre les déclarations. Ce formulaire doit aider à la rédaction d'une déclaration d'incident, en prévoyant des cases pour les informations demandées.

Pour faciliter la lecture par le personnel d'astreinte, copiez le contenu de la déclaration, en particulier le formulaire dans *le corps du mail* plutôt que d'utiliser des pièces jointes.

L'opérateur, peut, s'il l'estime utile, compléter les informations contenues dans le formulaire avec des éléments externes. À titre d'exemple, nous indiquons :

- une carte de la zone impactée par l'incident,
- un rapport d'incident interne,
- carte météo si l'incident est lié à un évènement météo, …

5. QUAND ENVOYER UNE DÉCLARATION ?

Déclaration initiale - Dès que les seuils et délais précisés dans le **Tableau 2** sont atteints, l'opérateur adresse une déclaration d'incident. L'opérateur dispose d'un délai de 15 minutes après le franchissement du seuil pour établir la déclaration.

Lors de la déclaration initiale, l'opérateur alerte les autorités de la survenue d'un incident en cours et fournit les informations disponibles au moment de la déclaration.

L'opérateur définit une référence d'incident qui sera réutilisée pour les déclarations ultérieures : mises à jour ou de clôture.

> **IMPORTANT :** Les durées d'indisponibilité mentionnées dans le Tableau **2** ont été établies pour laisser aux opérateurs le temps nécessaire pour détecter puis analyser l'incident. Néanmoins, en cas d'un incident exceptionnel par son ampleur, et en particulier si l'incident touche les communications d'urgence, l'opérateur doit établir une déclaration d'incident « dès qu'il en a connaissance ».

Déclaration de mise à jour - Comme il n'est pas toujours possible de disposer des informations précises ou complètes dès la déclaration initiale, l'opérateur effectuera des mises à jour selon le même modèle, en faisant référence au même incident et précisera les éléments utiles. Cette mise à jour pourra préciser les causes de l'incident, l'impact de l'incident, les mesures prises, ou les délais de rétablissement du service

Si la situation évolue (notamment lors d'un évènement climatique), et que les éléments de la déclaration initiale, ne sont plus à jour (notamment s'agissant de l'impact), l'opérateur adresse une actualisation en faisant référence à l'incident initial

Déclaration de clôture - Dès la fin de l'incident, une déclaration de clôture est établie selon la même procédure. Celle-ci actualise les informations, notamment les causes de l'incident et les mesures ayant permis d'y remédier. Cette déclaration de clôture est adressée aux mêmes destinataires que la déclaration initiale.

6. OÙ ENVOYER UNE DÉCLARATION ?

La procédure décrite ci-dessous doit être suivie pour toute déclaration initiale, mise à jour et clôture d'incident. Cette procédure est à suivre 24h/24 et 7 jours /7.

Pour tous les échanges avec l'administration, privilégier les échanges par mail, et éviter de contacter directement les autorités par téléphone sauf à leur demande. N'utiliser le téléphone comme premier contact que si la situation est critique et requiert l'attention immédiate de l'administration.

Tout incident d'intégrité correspondant aux critères de gravité mentionnés au chapitre 3 doit être déclaré au ministère de l'intérieur:

- Envoi d'un mail au COGIC
- **si l'incident est critique** : confirmer l'envoi par un appel téléphonique au centre de veille du COGIC

Tout incident de sécurité doit être déclaré conjointement au ministère de l'intérieur et à autorité nationale de défense des systèmes d'information

1. au ministère de l'intérieur
   - Envoi d'un mail au COGIC
   - **si l'incident est critique** : confirmer l'envoi par un appel téléphonique au centre de veille du COGIC
2. à l'autorité nationale de défense des systèmes d'information (ANSSI):
   - Envoi d'un mail au CERT-FR
   - **si l'incident est critique** : confirmer l'envoi par un appel téléphonique à la permanence opérationnelle du CERT-FR

   Attention : Le CERT-FR traite sur le plan technique les incidents concernant l'administration et les opérateurs d'importance vitale et de services essentiels. Le CERT-FR propose sur son site https://www.ssi.gouv.fr/en-cas-dincident/ des éléments pour avoir les bons réflexes en cas d'incident de sécurité.

Le mail envoyé aux administrations contiendra la déclaration d'incident en reprenant le modèle proposé en Annexe B : *Formulaire de déclaration d'incident*.

Les coordonnées des administrations sont confidentielles, et ne sont pas indiquées dans ce document. Pour les obtenir, vous devez suivre la procédure indiquée 9, *Demander l'annuaire des autorités à* informer

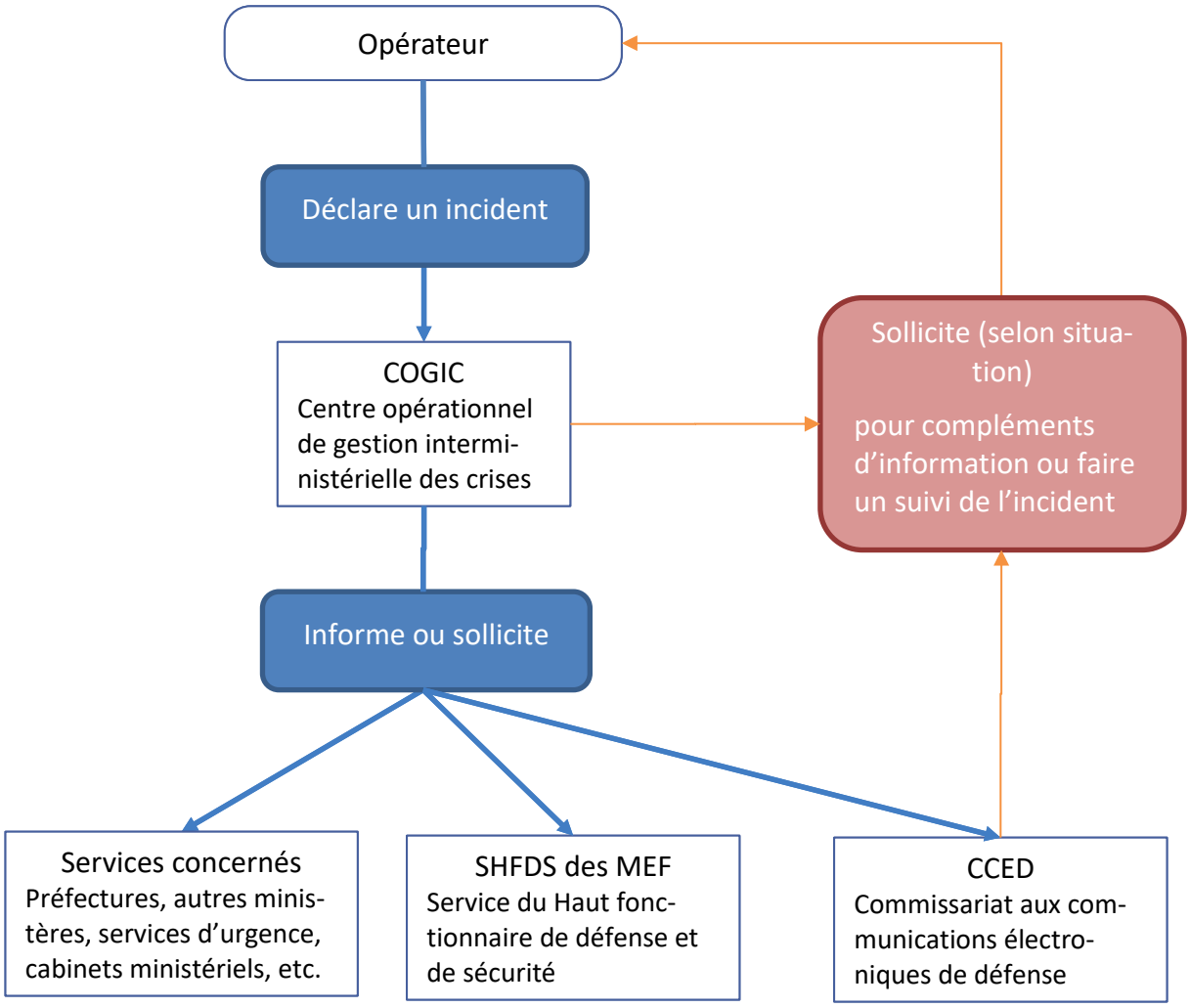
7. QUE SE PASSE-T-IL APRÈS LA DÉCLARATION ?

Dans tous les cas, à la réception d'une déclaration d'incident, le COGIC informe par mail les différents services concernés par l'incident, dont la permanence du SHFDS et le CCED. Si l'incident ne nécessite pas l'attention de l'administration, alors, l'opérateur est responsable de rétablir l'incident et d'envoyer une déclaration de clôture d'incident lorsque le service est rétabli.

Il arrive qu'un incident sorte de ce cadre simple. Le CCED peut être sollicité par le COGIC pour obtenir son avis sur un incident et pour obtenir des informations complémentaires auprès des opérateurs.

Enfin, si la situation le requiert, le COGIC ou le CCED pourront contacter l'opérateur à l'origine de la déclaration d'incident. Ce cas se présente si les autorités ont besoin de clarifier la nature de l'incident, d'en préciser les conséquences ou d'évaluer sa gravité, d'établir une prévision de retour en situation nominale,…

Figure 1 : Circuit d'envoi des déclarations d'incident



8. RETOUR D'EXPÉRIENCE APRÈS UN INCIDENT

Après la résolution de l'incident, qu'il soit lié à la sécurité ou à l'intégrité du réseau, le CCED peut demander à l'opérateur, en liaison avec le SHFDS des MEF, d'organiser dans ses locaux, au plus près des spécialistes, une réunion de retour d'expérience sur l'incident. Le but est d'en comprendre la genèse, de se faire présenter le cas échéant le plan d'actions que mettra en place l'opérateur mais aussi d'en tirer des enseignements pour les autres opérateurs. L'ANSSI est invitée à cette réunion de retour d'expérience[5].

En tant que de besoin, le ministère de l'intérieur (DGSCGC/COGIC) et l'ANSSI communiquent leur retour d'expérience en vue de l'amélioration des procédures.

9. DEMANDER L'ANNUAIRE DES AUTORITÉS À INFORMER

Les coordonnées des administrations à informer en cas d'incident sont restreintes, et ne sont pas indiquées dans ce document qui est ouvert au grand public.

Pour obtenir ces coordonnées, vous devez vous faire connaître comme opérateur par le CCED et le SHFDS. Pour cela :

- Envoyer un mail au CCED (adresse dans le tableau ci-dessous),
- Expliquer les raisons de votre demande

Le CCED prendra contact avec vous pour instruire votre demande et vérifier que vous êtes légitimes pour émettre des déclarations et recevoir les coordonnées des administrations.

Ministère	Autorité	Adresse mél.
MEF	CCED	incidents-cced.dge@finances.gouv.fr

10. DEMANDER UNE ÉVOLUTION DU GUIDE

Ce guide a vocation à évoluer pour tenir compte de l'expérience acquise, des évolutions légales ou réglementaires, de la nature des opérateurs susceptibles de déclarer des incidents. Les utilisateurs, qu'ils soient émetteurs potentiels de déclarations d'incident ou destinataires de ces déclarations, peuvent proposer des évolutions du guide.

Les demandes d'évolution sont à transmettre au CCED par mail, en précisant dans l'objet « *Modification du Guide de déclaration des incident* ».

Ministère	Autorité	Adresse mél.
MEF	CCED	incidents-cced.dge@finances.gouv.fr

5 Pour les incidents relevant d'un traitement au titre de l'article 34 de la LPM, l'ANSSI peut être l'initiateur de la réunion de retour d'expérience et dans ce cas invite le CCED et le SHFDS en tant que de besoin à cette réunion.

Annexe A. Contexte réglementaire

Extrait de l'article L. 33-14 du CPCE

Article L. 33-14 du code des postes et des communications électroniques[6] :

« […] Lorsque sont détectés des événements susceptibles d'affecter la sécurité des systèmes d'information, les opérateurs de communications électroniques en informent sans délai l'autorité nationale de sécurité des systèmes d'information. […] »

Extrait de l'article D. 98-5 du CPCE

Article D. 98-5 du code des postes et des communications électroniques[7] :

« III. – Sécurité des réseaux et des services.

[…] Dès qu'il en a connaissance, l'opérateur informe le ministre de l'intérieur de tout incident de sécurité ayant un impact significatif sur le fonctionnement de ses réseaux ou de ses services. Ce dernier en informe le ministre chargé des communications électroniques ainsi que les services de secours et de sécurité susceptibles d'être concernés. Lorsque l'atteinte à la sécurité résulte ou est susceptible de résulter d'un incident d'origine informatique, l'opérateur en informe également l'autorité nationale de défense des systèmes d'information. L'opérateur se conforme, le cas échéant, aux prescriptions techniques requises par le ministre chargé des communications électroniques pour remédier ou prévenir l'incident de sécurité.

Le caractère significatif de l'impact de l'incident de sécurité est déterminé en particulier au regard des paramètres suivants :

a) Le nombre d'utilisateurs touchés par l'incident de sécurité ;
b) La durée de l'incident de sécurité ;
c) L'étendue géographique de la zone touchée par l'incident de sécurité ;
d) La mesure dans laquelle le fonctionnement du réseau ou du service est affecté ;
e) L'ampleur de l'impact sur les activités économiques et sociétales.

Dès que l'opérateur a mené une analyse des causes et des conséquences de l'incident de sécurité, il en rend compte au ministre chargé des communications électroniques et à l'autorité nationale de défense des systèmes d'information dans le cas où cette dernière avait été informée ainsi que des mesures prises pour éviter leur renouvellement. Le ministre chargé des communications électroniques en informe les ministres intéressés. […] »

[6] Texte en vigueur à la date de publication de la présente version du guide
[7] Texte en vigueur à la date de publication de la présente version du guide

Annexe B. Formulaire de déclaration d'incident

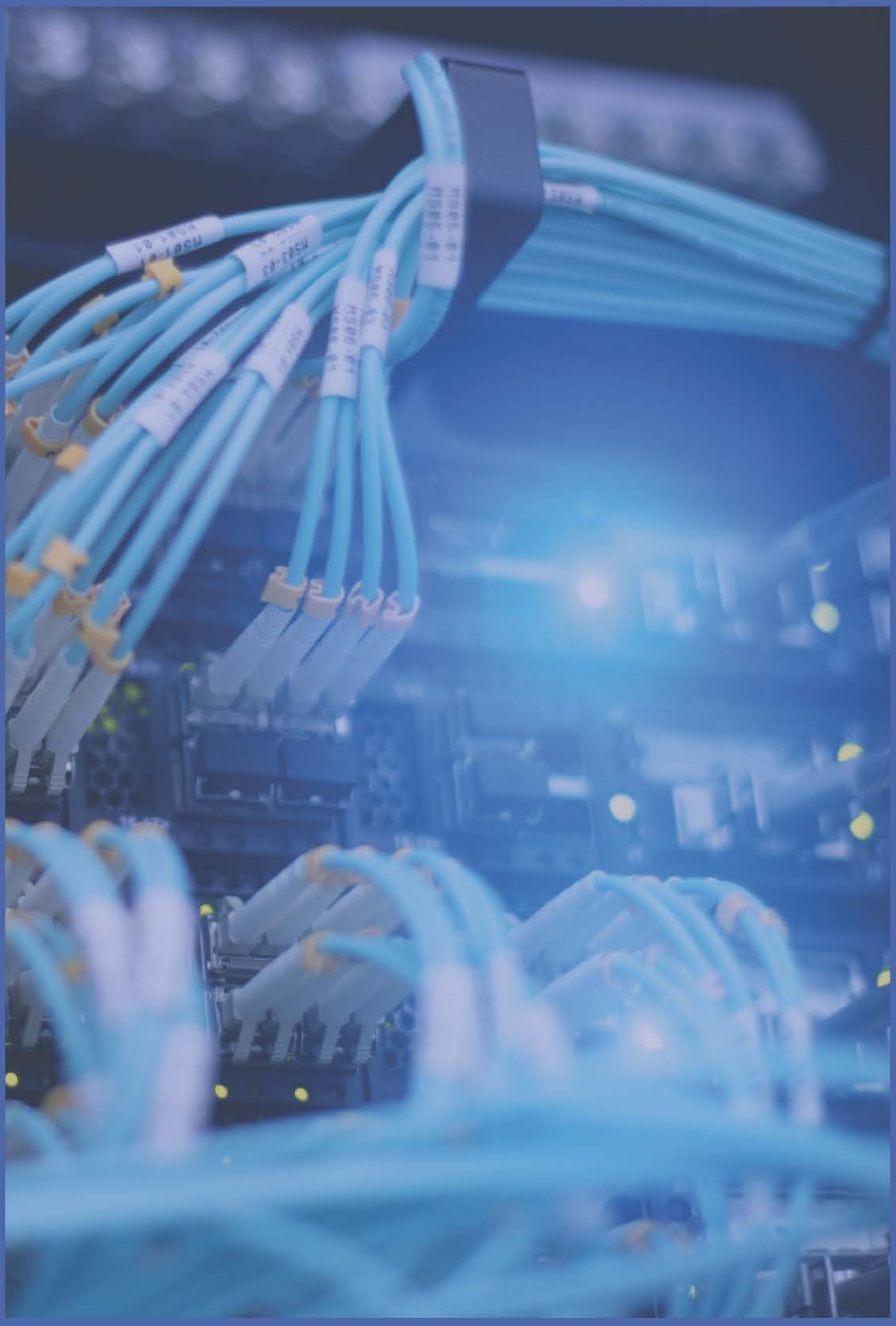
Référence	[Opérateur]_[COGIC/Cert-fr]_[Date]_[Heure déclaration]			
Déclaration	☐ Ouverture	☐ Mise à jour	☐ Clôture	
	Date	date.	**Heure**	hh :mm.
Déclarant	**Opérateur**	entrer le nom de l'opérateur		
(personne à contacter sur l'incident)	**M (me)**	entrer Nom/prénom		
	Titre	Titre/Fonction		
	Tél.	Téléphone	**Portable**	Portable
	Mail	Adresse Mail		
Descriptif de l'incident	Entrer ici la nature et l'origine présumée de l'incident. Lors d'une mise à jour, mettre à jour le descriptif			

Services impacté par l'incident	**Téléphonie**	**Urgences**	**Systèmes essentiels**	**Autres services**
	☐ Fixe ☐ Mobile ☐ Autre	☐ Téléphone ☐ Localisation ☐ Autre	☐ Interco voix ☐ Interco IP ☐ Autre	☐ Hébergement web ☐ Accès Internet ☐ Autre

Évaluation de l'impact de l'incident	Estimation du nbr abonnés. nb sites radios touchés. Localisation et étendue de la zone concernée par l'incident Toute autre observation utile pour décrire l'impact de l'incident, en précisant les conséquences sur les appels d'urgence.
Mesures prises	Description des investigations, interventions, des contournements en cours….
Évolution prévisible	Délai de rétablissement envisageable à ce stade, stabilisation/ extension de l'incident, résolution en cours, etc.
Observation	Proposition de mesure conservatoire à prendre par l'administration, de consignes à donner aux usagers, contact privilégié sur l'incident…

Annexe C. Glossaire

ANSSI	Agence nationale de la sécurité des systèmes d'information
ARCEP	Autorité de régulation des communications électroniques et des postes
CCED	Commissariat aux communications électroniques de défense
CERT	Sigle anglais pour « Computer Emergency Response Team »
CERT-FR	Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
CICRESCE	Commission interministérielle de coordination des réseaux et des services de communications électroniques pour la défense et la sécurité publique
COGIC	Centre opérationnel de gestion interministérielle de crise
COSSI	Centre opérationnel de la sécurité des systèmes d'information
CPCE	Code des postes et des communications électroniques
DGSCGC	Direction générale de la sécurité civile et de la gestion des crises
LPM	Loi de programmation militaire
MEF	Ministères économiques et financiers
PSAP	« Public Safety Answering Point » (Centre de réception des appels d'urgence)
SHFDS	Service du Haut Fonctionnaire de défense et de sécurité
SHFDS des MEF	SHFDS des ministères économiques et financiers



Crédit photo : 1re et 4e de couverture : ©Funtap - stock.adobe.com