

RÉSILIENCE NUMÉRIQUE

ANTICIPER, RÉSISTER ET REBONDIR

EDITO

Faire de la résilience numérique un réflexe de gouvernance est désormais une nécessité pour toutes les entreprises. Cette conviction est au cœur de ce guide. Elle s'impose avec d'autant plus de force dans un environnement où les dépendances numériques se multiplient et où une cyberattaque peut, en quelques heures, désorganiser profondément une activité.

Dans un contexte où l'innovation accélère, où les tensions géopolitiques se durcissent et où les attaques cyber sont toujours plus sophistiquées, nos entreprises doivent pouvoir continuer à fonctionner, à décider et à se projeter. Résister, absorber le choc, reprendre rapidement son activité : voilà ce que doit permettre une véritable démarche de résilience numérique.

Lorsqu'un incident survient, il ne concerne jamais seulement les systèmes d'information. Il affecte également l'organisation, les équipes, les clients et, plus largement, la confiance qui fonde l'activité de l'entreprise.

C'est pourquoi la résilience numérique ne peut être considérée comme un sujet technique parmi d'autres. Elle est un enjeu de direction, de compétitivité et de souveraineté. Elle suppose d'évaluer avec lucidité ses vulnérabilités et ses dépendances.



VIRGINIE FAUVEL

CEO, HARVEST

CO-PRÉSIDENTE, COMMISSION NUMÉRIQUE ET INNOVATION, MEDEF

Le MEDEF porte ce sujet depuis de nombreuses années : nous défendons une approche qui combine exigence de sécurité et pragmatisme économique. Ce guide s'inscrit dans cette ambition. Il ne prétend pas apporter une réponse uniforme à des réalités d'entreprise différentes, mais il vise à donner des repères, susciter les bons réflexes et, surtout, à encourager le passage à l'action.

Au sein de la Commission Numérique et Innovation du MEDEF, comme à l'occasion du Tour de la résilience, co-organisé avec Numeum et les fédérations volontaires, nous continuerons à porter cette conviction avec constance et exigence : la résilience numérique est désormais une condition essentielle de la performance et de la liberté d'entreprendre.

AVANT-PROPOS

- **Une entreprise numériquement résiliente n'est pas une entreprise qui ne connaît jamais d'incident.** C'est une entreprise qui connaît ses dépendances, anticipe les situations de crise, limite les conséquences d'une défaillance numérique, maintient ses activités essentielles et dispose des capacités nécessaires pour reprendre rapidement son fonctionnement.
- **La résilience numérique dépasse ainsi la seule protection des systèmes d'information.** Elle concerne l'organisation de l'entreprise, ses collaborateurs, ses ressources financières, ses obligations juridiques, ses relations contractuelles et l'ensemble de son écosystème.
- Ce guide propose **une approche de la résilience numérique, structurée autour de quatre piliers complémentaires.** Il vise à aider chaque entreprise, quels que soient sa taille, son secteur ou son niveau de maturité, à identifier ses vulnérabilités et à engager une démarche progressive et proportionnée de résilience numérique.



INTRODUCTION

COMPRENDRE LA RÉSILIENCE NUMÉRIQUE

1.1 Pourquoi la résilience numérique est devenue un enjeu pour les entreprises

La transformation numérique a profondément modifié le fonctionnement des entreprises. Les activités de production, de vente, de gestion ou de relation client reposent désormais sur des systèmes d'information, des logiciels, des données et des infrastructures interconnectées. Cette dépendance croissante au numérique constitue un facteur de performance, mais elle expose également les organisations à de nouveaux risques de rupture.

Une interruption du système d'information ne constitue plus seulement un incident technique isolé. Elle peut immédiatement affecter la capacité de l'entreprise à produire, facturer, livrer, payer ses salariés, communiquer avec ses clients ou respecter ses engagements contractuels. Dans les organisations les plus dépendantes du numérique, quelques heures d'indisponibilité peuvent suffire à désorganiser l'activité, à provoquer des pertes financières importantes.

La résilience numérique est ainsi devenue un enjeu transversal, qui concerne la direction générale autant que les fonctions informatiques.

Les incidents numériques ne sont pas uniquement liés aux cyberattaques. Ils peuvent résulter de causes très diverses : une panne matérielle ou logicielle ; une défaillance électrique ou de télécommunications ; un sinistre affectant les locaux ou les infrastructures ; une attaque informatique ; une défaillance dans la chaîne de sous-traitance, etc.

Cette diversité impose de ne pas limiter la résilience numérique à la lutte contre les actes malveillants. Une entreprise peut subir les mêmes conséquences opérationnelles à la suite d'une cyberattaque, d'une panne chez un fournisseur ou d'une erreur humaine. La démarche de résilience doit donc être construite à partir des impacts potentiels sur l'activité, et non uniquement à partir de l'origine de l'incident.

1.2 De la protection du système d'information à la continuité de l'entreprise

La résilience numérique désigne la capacité d'une organisation à anticiper les incidents affectant son environnement numérique, à en limiter les conséquences, à maintenir ses activités essentielles, puis à restaurer ses services dans des délais compatibles avec ses besoins. Elle comprend également la capacité à tirer les enseignements d'un incident afin de renforcer durablement l'organisation, ses processus et ses systèmes.

Une entreprise résiliente n'est donc pas une entreprise qui ne subit jamais de défaillance. Aucun dispositif technique ne permet de supprimer totalement le risque. La résilience consiste plutôt à empêcher qu'un incident numérique ne se transforme en interruption durable de l'activité, en perte irréversible de données ou en crise mettant en cause la pérennité de l'entreprise.

Cette approche dépasse la seule protection du système d'information. Elle concerne la continuité de la production, des ventes, de la facturation, de la logistique, de la relation client, du paiement des salariés ou encore du respect des obligations réglementaires. Le règlement européen DORA définit ainsi la résilience opérationnelle numérique comme **la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations.**

La résilience numérique rassemble différentes dimensions dans une démarche cohérente : elle associe la prévention, la protection, la détection, la réponse à incident, la continuité, la reconstruction et l'amélioration continue. La directive NIS 2 traduit cette approche globale en imposant aux entités concernées des mesures techniques, opérationnelles et organisationnelles proportionnées aux risques, incluant notamment la gestion des incidents, la continuité d'activité, la sécurité des fournisseurs et la gestion de crise.

1.3 Les capacités constitutives de la résilience

GOUVERNER

L'entreprise définit une politique de résilience, désigne les responsables et précise les niveaux de décision. Les directions métiers, la direction générale, la direction des systèmes d'information, la cybersécurité, les ressources humaines, la communication et les fonctions juridiques doivent connaître leur rôle.

EVALUER

L'organisation recense ses actifs, ses activités critiques, ses dépendances et les scénarios susceptibles de les interrompre. Cette analyse doit être complétée par une analyse d'impact sur l'activité, souvent appelée *Business Impact Analysis* (BIA). Celle-ci permet d'évaluer les conséquences d'une interruption dans le temps et de déterminer les priorités de continuité et de reprise.

PROTEGER

L'entreprise déploie des mesures destinées à réduire la probabilité qu'un incident survienne ou à en limiter immédiatement l'étendue : authentification multi-facteur, gestion des correctifs, cloisonnement des réseaux, limitation des privilèges, sécurisation des accès distants, chiffrement, journalisation, filtrage ou encore durcissement des configurations. Les mesures doivent être proportionnées à la criticité des activités et non appliquées de manière uniforme. Un système supportant une activité vitale ne peut pas être protégé selon les mêmes exigences qu'un outil secondaire.

RECONSTRUIRE

L'entreprise doit pouvoir maintenir un niveau de service minimal pendant la crise, puis restaurer ses capacités dans un ordre cohérent. Les plans doivent préciser les modes de fonctionnement dégradés, les solutions de repli, les ressources nécessaires, les procédures manuelles temporaires et les conditions de retour à la normale. L'ANSSI structure ainsi la préparation aux crises cyber autour de la gouvernance, des processus, de la communication, de la réponse à incident, de la continuité d'activité et de la reconstruction.

APPRENDRE

Après un incident ou un exercice, l'organisation réalise un retour d'expérience. Elle identifie les vulnérabilités, les décisions tardives, les dépendances mal maîtrisées et les procédures inadaptées. Les plans, architectures et contrats doivent ensuite être mis à jour. Une démarche de résilience est nécessairement continue : elle évolue avec les activités de l'entreprise, les outils utilisés, les fournisseurs et les menaces.

1.4 Quelques notions pour mesurer les besoins de continuité et de reprise

La résilience doit être traduite en objectifs mesurables. Sans objectifs explicites, il est impossible de déterminer si les dispositifs techniques et organisationnels sont suffisants. L'analyse d'impact doit notamment permettre de définir :

- **La durée maximale d'interruption admissible** : Elle correspond à la durée au-delà de laquelle l'interruption d'une activité provoque des conséquences jugées inacceptables pour l'entreprise.
- **L'objectif de délai de reprise** : Le Recovery Time Objective désigne le délai cible dans lequel un système ou un service doit être remis en fonctionnement. Techniquement, le RTO devrait être inférieur à la DMIA afin de conserver une marge pour la remise en service des processus métiers. Certains référentiels rapprochent néanmoins les deux notions : il convient donc de préciser les définitions retenues par l'entreprise pour éviter toute ambiguïté.
- **La perte de données maximale admissible (PDMA ou RPO)** : Elle définit le volume de données que l'entreprise peut accepter de perdre, exprimé sous forme de durée. Un RPO de quatre heures signifie que la restauration peut conduire à perdre jusqu'à quatre heures de données produites depuis la dernière sauvegarde exploitable.
- **Le niveau minimal de service** : Il précise le volume d'activité ou les fonctionnalités devant être maintenus pendant la crise. Une activité peut, par exemple, fonctionner avec un nombre réduit d'utilisateurs, uniquement pour certains clients ou à partir de procédures manuelles.



PILIER 1

GOUVERNANCE ET ORGANISATION

2.1 Faire de la résilience numérique une responsabilité de direction

La résilience numérique ne peut pas reposer uniquement sur la direction des systèmes d'information ou sur le responsable de la sécurité des systèmes d'information. Un incident numérique majeur affecte rapidement l'ensemble de l'entreprise : production, ventes, logistique, relation client, ressources humaines, finances, communication, obligations contractuelles et réglementaires.

Les décisions prises en situation de crise dépassent donc le seul champ technique : elles peuvent conduire à interrompre une activité, isoler une partie du système d'information, informer des clients, mobiliser des prestataires, notifier une autorité ou basculer vers un fonctionnement dégradé. Ces arbitrages relèvent de la gouvernance de l'entreprise et doivent être préparés avant la survenue d'un incident.

La direction générale doit ainsi définir le niveau de risque acceptable, fixer les priorités de continuité, et s'assurer que les moyens humains, techniques et financiers sont cohérents avec les besoins de l'organisation.



LA RÉSILIENCE NUMÉRIQUE EST UNE RESPONSABILITÉ COLLECTIVE, PILOTÉE AU PLUS HAUT NIVEAU DE L'ENTREPRISE.

2.2 Quelques pistes pour amorcer la réflexion

La première étape consiste à déterminer les activités dont l'interruption provoquerait les conséquences les plus importantes pour l'entreprise. Il ne s'agit pas seulement de recenser les applications informatiques, mais d'identifier les processus métiers essentiels à la continuité de l'activité.

Cette analyse doit permettre d'évaluer les conséquences d'une interruption dans le temps : après quelques heures, une journée, plusieurs jours ou plusieurs semaines. Les impacts doivent être examinés sous plusieurs angles : financier, opérationnel, juridique, humain, commercial et réputationnel.

L'entreprise peut formaliser cette démarche au moyen d'une analyse d'impact sur l'activité, ou *Business Impact Analysis*. Pour débiter, la méthode EBIOS Risk Manager peut alimenter la démarche de résilience.



ZOOM SUR : LA MÉTHODE EBIOS RISK MANAGER



2.3 Définir une gouvernance des risques numériques

Les risques numériques doivent être intégrés au dispositif général de gestion des risques de l'entreprise. Ils ne doivent pas être suivis séparément des risques financiers, industriels, juridiques, humains ou opérationnels, car un même incident peut produire des conséquences dans l'ensemble de ces domaines.

La gouvernance doit permettre de répondre à plusieurs questions, parmi lesquelles :

- quels sont les principaux scénarios de rupture numérique ;
- quelles activités seraient affectées ;
- quel niveau d'interruption est acceptable ;
- quelles mesures doivent être financées en priorité ;
- quels risques peuvent être acceptés, réduits, transférés ou évités ;
- comment les incidents et les exercices donnent-ils lieu à des actions correctrices.

Selon la taille de l'organisation, cette gouvernance peut être assurée par un comité dédié ou intégrée à un comité des risques, un comité de direction, un comité d'audit ou une instance de sécurité des systèmes d'information. L'objectif n'est pas de multiplier les tableaux de bord, mais de fournir à la direction une vision suffisamment claire pour prendre des décisions et arbitrer les investissements.

2.4 Répartir clairement les responsabilités

Question structurante : Qui décide, qui agit et qui communique lorsque les outils numériques ne sont plus disponibles ?

La répartition des rôles peut être formalisée au moyen d'une **matrice de responsabilités de type RACI** :

- **Responsible** : la personne ou l'équipe qui réalise l'action ;
- **Accountable** : la personne qui prend la décision et en assume la responsabilité ;
- **Consulted** : les fonctions dont l'avis est requis ;
- **Informed** : les personnes qui doivent être informées.

Les rôles doivent être attribués nominativement ou par fonction, avec des suppléants identifiés. Une responsabilité qui n'est attribuée qu'à une seule personne crée un point de fragilité, notamment en dehors des horaires habituels, pendant les congés ou lorsque cette personne est elle-même indisponible.

PILIER 2

CONTINUITÉ OPERATIONNELLE

3.1 Le plan de continuité d'activité (PCA) et le plan de reprise d'activité (PRA)

Le **plan de continuité d'activité (PCA)** organise le maintien des activités essentielles pendant l'incident. Il précise les modes de fonctionnement dégradés qui peuvent être activés lorsque les outils numériques habituels ne sont plus disponibles.

Le **plan de reprise d'activité (PRA)** organise la restauration des systèmes d'information et des services numériques après une interruption.

Le PCA et le PRA ne doivent pas être conçus séparément. Le PCA exprime les besoins de continuité des métiers ; le PRA traduit ces besoins en priorités et solutions techniques.



ZOOM SUR : GUIDE SGDSN POUR REALISER UN PCA





PILIER 3

HUMAIN ET CULTURE DE LA RÉSILIENCE

4.1 Faire des collaborateurs un maillon actif de la résilience

La résilience numérique repose autant sur les capacités humaines et organisationnelles de l'entreprise que sur la robustesse de ses systèmes techniques.

Le facteur humain est souvent présenté comme une vulnérabilité : erreur de manipulation, mot de passe compromis, ouverture d'une pièce jointe malveillante ou contournement d'une procédure. Cette lecture est incomplète. Les collaborateurs constituent également la première capacité de détection et de réaction de l'entreprise. Un comportement inhabituel identifié rapidement, un signalement transmis au bon interlocuteur ou une équipe capable de poursuivre son activité en mode dégradé peuvent limiter fortement les conséquences d'un incident.

L'enjeu consiste donc à passer d'une logique de sensibilisation ponctuelle à une véritable culture de la résilience, dans laquelle chaque collaborateur connaît son rôle, comprend les risques liés à son activité et sait comment agir lorsque les outils numériques habituels ne sont plus disponibles.



LES COLLABORATEURS PEUVENT ÊTRE À L'ORIGINE D'UN INCIDENT, MAIS ILS SONT SURTOUT LES PREMIERS ACTEURS DE SA DÉTECTION, DE SA GESTION ET DE SA RÉOLUTION.

4.2 Adapter les formations aux fonctions et responsabilités

Les collaborateurs n'ont ni les mêmes usages numériques, ni la même exposition aux risques, ni les mêmes responsabilités en situation de crise. La formation doit donc être adaptée et différenciée selon les fonctions exercées et les décisions susceptibles d'être prises.

Un socle commun pour l'ensemble des collaborateurs : Chaque collaborateur doit connaître les règles essentielles de sécurité et être capable de reconnaître une situation inhabituelle : message suspect, comportement anormal d'un poste de travail, perte d'un équipement, demande inhabituelle de transfert financier, etc. Il doit surtout savoir quoi faire immédiatement : arrêter une action, conserver les éléments utiles, contacter le bon interlocuteur et éviter les manipulations susceptibles d'aggraver la situation.

La formation doit ainsi associer connaissance du risque et capacité d'action.

Une préparation spécifique des fonctions de crise : Les membres susceptibles d'intégrer une cellule de crise doivent être préparés à des tâches différentes de leurs missions quotidiennes : qualification d'une situation incertaine, arbitrage entre plusieurs options imparfaites, maintien d'une activité dégradée, notification aux autorités, communication avec les salariés ou gestion de la pression externe. Un dirigeant n'a pas besoin de savoir administrer un pare-feu. Il doit en revanche être capable de comprendre les conséquences d'une décision technique : faut-il isoler immédiatement une infrastructure au risque d'interrompre la production ? Quand faut-il activer le PCA ?

La formation doit donc être conçue en fonction des décisions attendues, et non uniquement des connaissances techniques.

4.3 Intégrer la résilience dans le cycle de vie des collaborateurs

La gestion des arrivées, mobilités et départs constitue un élément important de la résilience numérique.

- **Lorsqu'un collaborateur rejoint l'entreprise**, ses accès doivent être attribués selon ses besoins réels, ses responsabilités doivent être précisées et les règles essentielles de sécurité doivent lui être présentées dès son arrivée.
- **En cas de changement de poste**, les droits d'accès doivent être réévalués. L'accumulation de droits au fil des mobilités internes peut créer des privilèges excessifs ou maintenir des accès devenus inutiles.
- **Lors d'un départ**, les comptes et accès doivent être supprimés ou suspendus dans des délais maîtrisés. Les données, documents et responsabilités détenus par le collaborateur doivent également être transférés afin d'éviter qu'une information critique ne disparaisse avec son départ.

4.4 Faciliter le signalement des incidents

La vitesse de détection constitue un facteur déterminant dans la maîtrise d'un incident. Un événement signalé rapidement peut parfois être contenu avant qu'il ne touche une part importante du système d'information. La procédure de signalement doit donc être particulièrement simple.

Tout collaborateur doit pouvoir répondre à quatre questions :

QUE DOIS-JE SIGNALER ?

Un comportement inhabituel, une erreur susceptible d'avoir un impact, un équipement perdu, un message suspect, une indisponibilité anormale ou toute autre situation qui pourrait affecter le système d'information.

À QUI ?

Un interlocuteur clairement identifié : support informatique, équipe de sécurité, responsable hiérarchique ou dispositif dédié.

COMMENT ?

Au moyen d'un canal immédiatement accessible.

QUE DOIS-JE FAIRE EN ATTENDANT ?

Des consignes simples doivent préciser les actions à réaliser ou, au contraire, à éviter.

Le dispositif doit également rester opérationnel lorsque les moyens numériques habituels sont indisponibles. Une procédure de signalement accessible uniquement sur l'intranet ou par courrier électronique devient inutile lorsque ces systèmes constituent précisément la cible de l'incident.

L'entreprise doit donc prévoir au moins un canal alternatif : téléphone, numéro externe, messagerie de secours ou coordonnées conservées hors ligne.



LA CULTURE DE RÉSILIENCE REPOSE AINSI SUR UN PRINCIPE SIMPLE : SIGNALER RAPIDEMENT DOIT TOUJOURS ÊTRE PLUS FACILE ET PLUS SÛR QUE DISSIMULER UNE ERREUR.

Développer une « culture juste » de l'erreur : Encourager le signalement suppose également de créer les conditions permettant aux collaborateurs de reconnaître rapidement une erreur. Une politique systématiquement punitive peut produire un effet inverse à celui recherché : un collaborateur qui craint une sanction peut être tenté de masquer son erreur ou d'attendre avant de la signaler. Une organisation résiliente doit développer une culture juste, distinguant plusieurs situations : l'erreur involontaire commise malgré le respect des règles ; le comportement à risque adopté par facilité ou par méconnaissance ; la violation délibérée et répétée d'une règle connue...

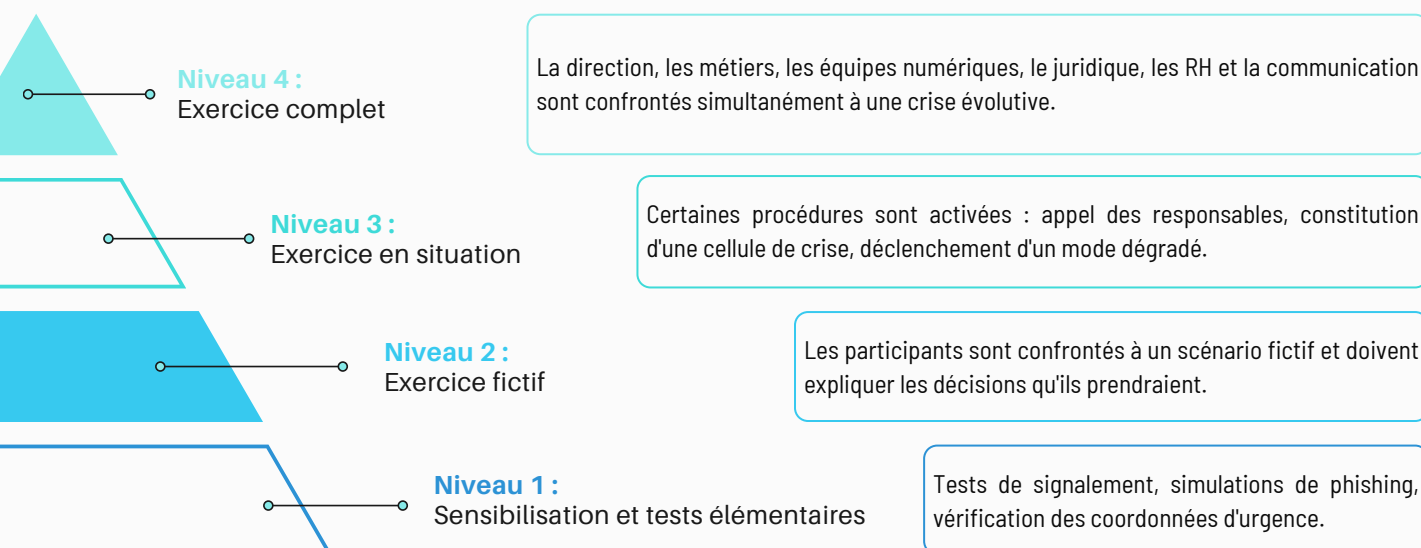
4.5 Entraîner les équipes par des exercices

Préparer les métiers à fonctionner sans leurs outils habituels : La résilience se mesure également à la capacité des collaborateurs à poursuivre leurs missions lorsque tout ou partie du système d'information devient indisponible. Cette situation doit être préparée avec les métiers : pour chaque activité critique, il convient d'identifier : les tâches qui doivent absolument être maintenues ; les données minimales nécessaires ; les personnes devant rester mobilisées ; les moyens alternatifs de communication et de validation.

Préparer les équipes à décider en environnement dégradé : Les crises numériques placent les équipes dans une situation particulière : l'information disponible est souvent incomplète, évolutive et parfois contradictoire. Les collaborateurs et responsables doivent donc être préparés à prendre des décisions sans disposer de leur environnement normal de travail (indisponibilité des outils collaboratifs, absence d'accès aux données, pression importante, forte incertitude sur la durée de l'incident...).

Dans ce contexte, la clarté des rôles et des délégations devient déterminante. Les équipes doivent savoir quelles décisions elles peuvent prendre de manière autonome, quelles décisions nécessitent un arbitrage et vers qui elles doivent les faire remonter. L'objectif est d'éviter deux situations opposées : une organisation paralysée dans l'attente d'une validation, ou une multiplication d'initiatives individuelles contradictoires.

Faire de l'entraînement une composante permanente de la résilience : La connaissance d'une procédure ne garantit pas la capacité à l'appliquer sous pression. L'entraînement doit permettre de transformer des procédures théoriques en automatismes collectifs. L'entreprise peut construire une progression allant du plus simple au plus complexe :



Un exercice réussi n'est pas nécessairement un exercice dans lequel aucune erreur n'a été commise.

C'est un exercice qui permet d'identifier les écarts entre ce que l'entreprise pensait pouvoir faire et ce qu'elle est effectivement capable de faire.

L'ANSSI recommande précisément de développer une stratégie d'amélioration continue par l'entraînement et propose différents formats, allant de la sensibilisation et des exercices sur table à des simulations plus complètes.

4.6 Organiser la communication interne de crise

Lorsque les outils habituels deviennent indisponibles ou non fiables, les collaborateurs cherchent naturellement des réponses. En l'absence de communication structurée, les informations partielles, les rumeurs ou les instructions contradictoires peuvent rapidement se multiplier.

L'entreprise doit donc anticiper la communication interne et prévoir des canaux indépendants des infrastructures susceptibles d'être affectées. Les messages diffusés doivent permettre aux collaborateurs de comprendre : la nature générale de la situation ; les actions qu'ils doivent effectuer ; les comportements à adopter ; le canal sur lequel seront communiquées les prochaines consignes. L'information doit être régulière, même lorsqu'aucune évolution majeure n'est intervenue.

La communication interne constitue ainsi une véritable mesure de maîtrise du risque : elle permet d'orienter les comportements collectifs et d'empêcher que les collaborateurs n'aggravent involontairement la situation.

4.7 Faire du retour d'expérience un outil de progression

Deux temps peuvent être distingués :

RETEX A CHAUD

Organisé rapidement après l'exercice ou l'incident, permet de recueillir les impressions et difficultés encore présentes dans la mémoire des participants.

RETEX A FROID

Réalisé après analyse, permet d'identifier les causes structurelles et de transformer les constats en actions correctrices.

Chaque action doit ensuite être attribuée à un responsable, disposer d'une échéance et être suivie jusqu'à sa clôture. Sans ce suivi, le retex risque de devenir un document supplémentaire sans impact réel sur la résilience.

Les ressources d'exercice publiées par l'ANSSI prévoient d'ailleurs explicitement des dispositifs de débriefing, de retex à chaud et à froid, des grilles d'observation et des relevés d'actions.

Ces enseignements doivent ensuite être intégrés dans les formations, procédures, plans de continuité et exercices futurs.



ZOOM SUR LES RESSOURCES D'EXERCICE ANSSI



Quelques questions à se poser :

- Les formations sont-elles adaptées aux fonctions et aux responsabilités ?
- Les nouveaux collaborateurs reçoivent-ils les consignes essentielles dès leur arrivée ?
- Les accès sont-ils correctement modifiés ou supprimés lors des mobilités et départs ?
- Les collaborateurs savent-ils comment signaler rapidement un incident ?
- Un canal de signalement reste-t-il disponible si la messagerie est indisponible ?
- Les erreurs peuvent-elles être signalées sans crainte d'une sanction automatique ?
- Les personnes et compétences critiques sont-elles identifiées ?
- Les procédures de mode dégradé ont-elles déjà été testées ?
- Des moyens de communication alternatifs sont-ils prévus ?
- Les incidents/exercices donnent-ils systématiquement lieu à un retour d'expérience ?



UNE CULTURE DE RÉSILIENCE SE CONSTRUIT PAR CETTE CAPACITÉ COLLECTIVE À APPRENDRE DES INCIDENTS RÉELS COMME DES SIMULATIONS.



PILIER 4

JURIDIQUE ET RÉGLEMENTAIRE - ZOOM SUR NIS2

La directive européenne NIS2, dont la transposition est organisée en France par le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, marque un changement d'échelle. La cybersécurité devient un sujet de gouvernance, de continuité d'activité et de responsabilité pour plusieurs milliers d'organisations, et plus seulement pour les opérateurs historiquement considérés comme vitaux.



À la date du présent guide, la directive NIS2 est entrée en vigueur au niveau européen, **mais sa transposition française demeure en cours**. Le projet de loi a été adopté par le Sénat en première lecture le 12 mars 2025 puis examiné en commission spéciale à l'Assemblée nationale. Les règles nationales définitives, les décrets et certaines exigences techniques peuvent encore évoluer. **Les éléments présentés comme « projet français » doivent donc être confirmés lors de la promulgation.**

5.1 NIS2 en bref : ce que vous devez savoir

Comprendre NIS2 en cinq minutes. NIS2 poursuit trois objectifs : élever le niveau de cybersécurité dans l'Union européenne, réduire les écarts entre États membres et améliorer la coopération en cas de crise. Sa logique peut être résumée par quatre verbes : connaître, prévenir, détecter et réagir.

Connaître	Prévenir	Détecter	Réagir
Services, actifs, données, risques et dépendances	Mesures techniques, humaines, contractuelles et organisationnelles	Surveillance, journaux, alertes, signalement interne	Crise, continuité, restauration, notification et retour d'expérience

NIS2 est une réglementation fondée sur les risques. Elle ne prescrit pas un produit ou une architecture identique pour tous : les mesures doivent être appropriées et proportionnées au risque, à la taille de l'entité, à son exposition, à la gravité potentielle d'un incident et à l'état de l'art. Cette souplesse implique en contrepartie de pouvoir justifier ses choix.

CE QUE NIS2 CHANGE RÉELLEMENT

- Un périmètre élargi : 18 secteurs et, en France, environ 15 000 entités selon les estimations parlementaires.
- Une gouvernance renforcée : les organes de direction approuvent et supervisent les mesures de gestion des risques et doivent suivre une formation adaptée.
- Une approche couvrant l'ensemble de l'organisation : technique, métiers, RH, achats, juridique, communication et direction générale.
- Une attention explicite à la chaîne d'approvisionnement et aux prestataires de services.
- Des obligations de notification graduée des incidents significatifs.
- Une supervision et des sanctions différenciées entre entités essentielles et importantes.

5.2 Suis-je concerné par la directive NIS2

La catégorie dépend principalement du secteur, de la taille et de cas particuliers. La formulation simplifiée ci-dessous constitue un premier filtre, pas une décision juridique définitive.

La directive identifie deux types de secteurs : hautement critiques (Annexe I de la directive) et critiques (Annexe II de la directive).

- **Les secteurs hautement critiques** sont l'énergie, les transports, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, la gestion des services TIC, l'administration publique et l'espace.
- **Les secteurs critiques** sont les services postaux, la gestion des déchets, la fabrication de produits chimiques, l'agro-alimentaire, l'industrie manufacturière, les fournisseurs de services numériques et la recherche.

En plus des secteurs d'activités, les entreprises sont classées par taille :

Taille	Nb. employés		Chiffre d'affaires (millions d'€)		Bilan annuel (millions d'€)	Annexe I	Annexe II
Grandes	$x \geq 250$	OU	$y \geq 50$	ET	≥ 43	EE	EI
Moyennes	$50 \leq x \leq 250$		$10 \leq y \leq 50$		$10 \leq y \leq 43$	EI	EI
Micro & Petites	$x < 50$		$y < 10$		$z < 10$	Non concernées	

Attention : certains acteurs relèvent de règles particulières ou peuvent être qualifiés d'entités essentielles ou importantes indépendamment de ces seuils. La qualification doit également tenir compte de l'activité exacte exercée et des éventuelles désignations prévues par le projet de loi.

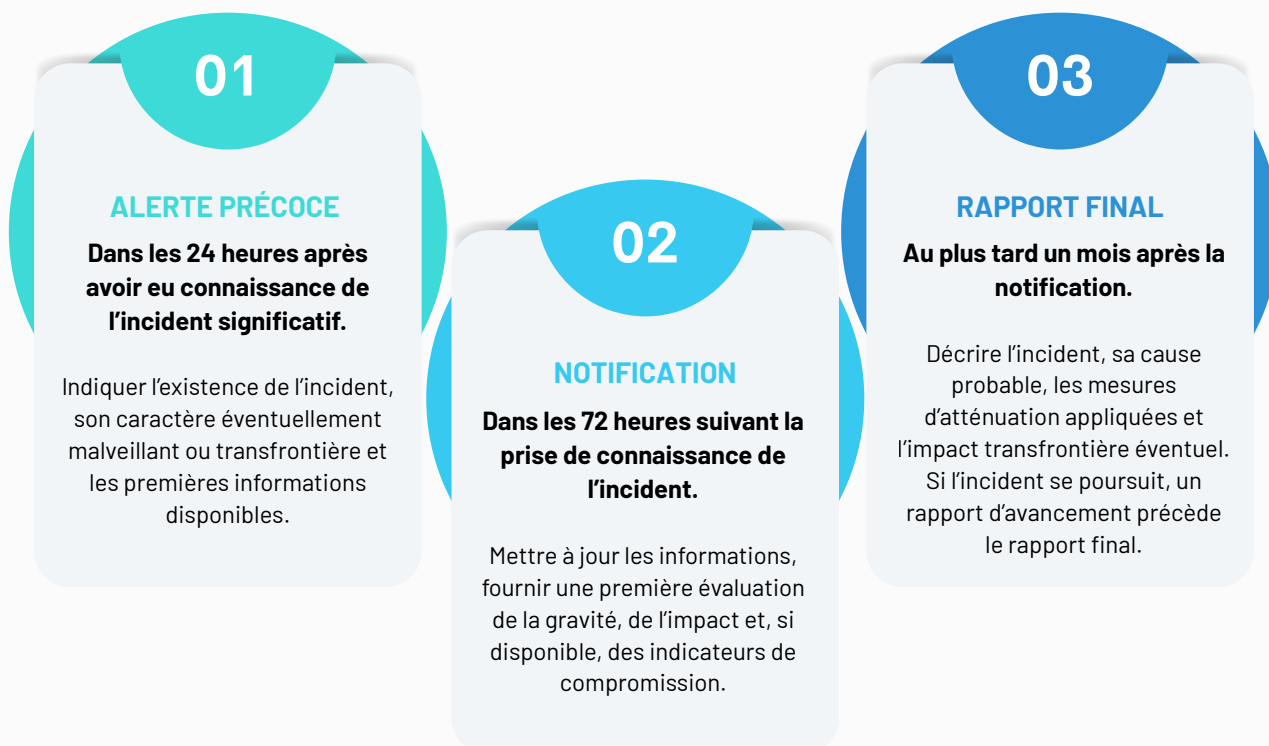
La catégorie dépend principalement du secteur, de la taille et de cas particuliers. La formulation simplifiée ci-dessous constitue un premier filtre, pas une décision juridique définitive.

Activité / taille	Grande entreprise	Entreprise moyenne	Petite ou microentreprise
Secteur hautement critique – annexe I	En principe : entité essentielle	En principe : entité importante	En principe : hors périmètre, sauf cas spécial ou désignation
Autre secteur critique – annexe II	En principe : entité importante	En principe : entité importante	En principe : hors périmètre, sauf cas spécial ou désignation
Cas spécifiques (ex. certains services DNS, confiance, communications électroniques)	Qualification particulière, parfois quelle que soit la taille	Qualification particulière	Peut être concernée quelle que soit la taille
Entité critique au titre de la directive REC	Entité essentielle	Entité essentielle	Entité essentielle

5.3 Les obligations principales

S'IDENTIFIER ET S'ENREGISTRER	Qualifier la personne morale, communiquer les informations requises à l'ANSSI et maintenir ces données à jour
GOUVERNER LES RISQUES	Approbation et supervision par la direction ; rôles, ressources, formation et reporting
GÉRER LES RISQUES	Mesures techniques, opérationnelles et organisationnelles proportionnées
NOTIFIER LES INCIDENTS	Détecter, qualifier, alerter et informer l'ANSSI selon un calendrier gradué
MAÎTRISER LES FOURNISSEURS	Évaluer les dépendances et risques de la chaîne d'approvisionnement
COOPÉRER AU CONTRÔLE	Répondre aux demandes, audits, inspections et prescriptions

Parmi les obligations, les entreprises sont tenues de notifier l'incident auprès de l'autorité compétente. Cette notification s'organise en trois grands moments :



Ce que signifie « notifier sous 24 h » : Il ne s'agit pas de fournir une analyse forensique complète en un jour. L'organisation doit pouvoir reconnaître qu'un incident peut être significatif, préserver les faits essentiels, mobiliser les décideurs et émettre une alerte précoce fiable. Les critères nationaux détaillés seront précisés par les textes d'application.

Une même attaque peut également déclencher d'autres obligations : violation de données personnelles auprès de la CNIL, déclaration à une autorité sectorielle, plainte, obligations contractuelles ou information des clients. Il faut coordonner les circuits sans supposer qu'une notification en remplace automatiquement une autre.

5.4 Un rôle renforcé pour le dirigeant

Les organes de direction doivent approuver les mesures de gestion des risques, superviser leur mise en œuvre et suivre une formation leur permettant de comprendre et d'évaluer les risques. La direction doit organiser une remontée d'information régulière et obtenir une vision claire des risques résiduels, des écarts et des arbitrages budgétaires.

5.5 Contrôles et sanctions

Les entités essentielles font l'objet d'une supervision plus proactive : inspections, audits, contrôles à distance, demandes d'information et analyses de preuves peuvent intervenir sans attendre un incident. Les entités importantes sont principalement supervisées a posteriori, lorsqu'existent des éléments laissant penser à un manquement. Cette différence ne réduit pas leurs obligations de fond.

Catégorie	Plafond retenu par le projet français	Lecture
Entité essentielle	Jusqu'à 10 M€ ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent – le montant le plus élevé	Plafond maximal prévu pour les personnes morales concernées ; sanction proportionnée au manquement et encadrée par la procédure nationale.
Entité importante	Jusqu'à 7 M€ ou 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent – le montant le plus élevé	Même logique de proportionnalité ; le calcul et l'entité économique de référence doivent être examinés précisément.

La sanction financière n'est pas le seul risque : mise en demeure, injonction, audit imposé, publicité d'un manquement, coûts de remédiation, responsabilité contractuelle, perte de clients et interruption d'activité peuvent être plus lourds. La directive prévoit que les circonstances, la gravité, la durée, les dommages, la coopération et les mesures prises soient pris en compte.



Pour les entreprises relevant de plusieurs cadres (RGPD, DORA, exigences sectorielles, sécurité des produits, obligations contractuelles), construire une matrice unique des obligations permet de mutualiser les preuves, les contrôles et les circuits de notification sans confondre les seuils ni les autorités compétentes.

RESSOURCES

PORTAIL OFFICIEL DE L'ANSSI - NIS2



SIMULATEUR NIS2 DE L'ANSSI



GUIDE D'HYGIENE INFORMATIQUE DE L'ANSSI



CYBERMALVEILLANCE.GOUV.FR



MALLETTE CYBER PRO



