ZERVAL

CODEX

ÉDITION DIRIGEANTS 2026

L'essentiel de la cybersécurité
pour comprendre, décider et agir

20 MINUTES POUR DÉCIDER

POUR LES DIRIGEANTS DE TPE, PME ET PETITES ORGANISATIONS

PRO.ZERVAL.IO

OUVRAGE

CODEX, Édition Dirigeants 2026

Une doctrine condensée pour décider sans devenir expert.

> **PROMESSE DE LECTURE**
> En vingt minutes, comprendre ce qui est en jeu, décider avant la crise et conserver la maîtrise pendant les premières heures.

À qui s'adresse ce livret

Ce livret s'adresse aux dirigeants de TPE, PME, collectivités, associations et cabinets. Il donne des repères d'arbitrage accessibles sans connaissances techniques particulières.

Édition et portée

Publié par DATASHIELD Risk Consulting, DRC SAS, sous la marque Zerval. Zerval PRO désigne l'environnement destiné aux organisations. Ce livret présente une doctrine générale. Il ne remplace ni un audit, ni une analyse de risques propre à votre organisation, ni un avis juridique. Les références ont été vérifiées au 24 août 2026.

Ce que la direction doit décider

QUESTION DE DIRECTION	DÉCISION ATTENDUE
Qu'est-ce qui doit continuer ?	Nommer trois à cinq missions vitales et leur durée d'interruption tolérable.
Quelles informations exigent le plus haut niveau de protection ?	Classer les données critiques et limiter leurs accès.
Que faisons-nous si un prestataire devient indisponible ?	Prévoir les rôles, les délais, les sauvegardes, la réversibilité et l'escalade.
Comment travaillons-nous une semaine sans informatique ?	Définir un mode dégradé réaliste et l'éprouver.
Qui décide pendant la crise ?	Nommer un directeur de crise, un suppléant et un circuit d'arbitrage court.

LECTURE

Comment utiliser ce livret

Trois parcours, selon le temps disponible.

01	5 minutes Lisez les ouvertures de parties, les encadrés Décision de direction et le mémento final.
02	20 minutes Suivez l'ordre : comprendre, gouverner, réagir, puis confronter les repères à votre organisation.
03	En comité de direction Utilisez les tableaux comme ordre du jour : missions vitales, dépendances, continuité, crise, notification et responsabilités.

Le fil conducteur

Le parcours part de la mission, organise les décisions à froid, garde la maîtrise pendant l'incident et transforme les principes en actions concrètes. L'ambition est volontairement resserrée : rendre les décisions essentielles plus claires.

Sommaire

PARTIE I

COMPRENDRE

Avant de protéger les outils, préciser ce que l'organisation doit préserver.

DÉCISION ET RESPONSABILITÉ

La cybersécurité relève de la direction

Vous n'avez pas à devenir technicien. Vous devez savoir ce qui est vital, fixer ce que l'organisation accepte de risquer et décider de ce qu'elle refuse de perdre.

Commencer par la mission

Les outils ne peuvent pas répondre aux questions de continuité, de confiance ou de responsabilité. La direction doit rendre les priorités explicites, attribuer les rôles, connaître les dépendances et garder une trace des arbitrages.

> **DÉCISION DE DIRECTION**
> Traitez la cybersécurité comme un sujet de continuité, de confiance et de responsabilité. Le budget informatique vient ensuite.

Ce qui est réellement exposé

Un incident peut arrêter la facturation ou la production, perturber la paie, rendre des dossiers indisponibles, exposer des informations confidentielles et fragiliser la confiance des équipes ou des clients. Les systèmes soutiennent ces activités. Ils ne constituent pas la finalité.

Posez une question simple : quelles activités doivent continuer malgré l'incertitude ? Remontez ensuite vers les données, les applications, les prestataires, les personnes et les équipements qui les rendent possibles.

MENACE OBSERVÉE

La menace réelle, sans surenchère

Les chiffres publics décrivent les incidents connus des autorités. Ils éclairent une tendance, sans prétendre mesurer toute la menace.

3 586 événements traités par l'ANSSI en 2025 [S01]	**1 366** incidents confirmés portés à sa connaissance [S01]
128 compromissions par rançongiciel recensées [S01]	**Hameçonnage** vecteur d'accès initial toujours majeur en Europe [S02]

Pourquoi les petites structures restent exposées

Les attaques opportunistes recherchent un accès facile : mot de passe réutilisé, service non corrigé, compte mal protégé ou fournisseur compromis. La taille offre peu de protection lorsque la surface visible reste accessible.

Dans le périmètre observé par l'ANSSI en 2025, les PME, TPE et ETI forment la catégorie la plus représentée parmi les victimes de rançongiciel. Une interruption de plusieurs jours y pèse souvent plus lourd, car les ressources de réponse et les solutions de repli sont limitées. [S01]

ARBITRAGE

Fixer le niveau de risque acceptable

Aucune organisation ne supprimera toute incertitude. La gouvernance sert à identifier les scénarios capables d'atteindre la mission, à réduire les plus graves et à assumer le risque résiduel en connaissance de cause.

Chaque risque accepté doit avoir un responsable, une justification et une date de réexamen. Sans ces trois éléments, l'organisation subit le risque au lieu de le gouverner.

> **DÉCISION DE DIRECTION**
> La direction prend des décisions proportionnées, documentées et assumées, même lorsque les informations restent incomplètes.

Trois questions immédiates

01	Mission Quelles activités doivent continuer lorsque les systèmes deviennent indisponibles ?
02	Confiance Quelles données ou décisions provoqueraient un dommage durable si elles étaient exposées ?
03	Tolérance Combien de temps l'organisation peut-elle fonctionner en mode dégradé ?

PARTIE II

GOUVERNER

Les décisions les moins coûteuses se prennent à froid, avant l'incident.

PRIORITÉS

Partir des missions, puis remonter vers les outils

Commencez par trois à cinq missions vitales. Pour chacune, identifiez les personnes, les données, les fournisseurs et les systèmes qui conditionnent sa continuité.

QUESTION DE DIRECTION	DÉCISION ATTENDUE
Qu'est-ce qui doit continuer ?	Nommer trois à cinq missions vitales et leur durée d'interruption tolérable.
Quelles informations exigent le plus haut niveau de protection ?	Classer les données critiques et limiter leurs accès.
Que faisons-nous si un prestataire devient indisponible ?	Prévoir les rôles, les délais, les sauvegardes, la réversibilité et l'escalade.
Comment travaillons-nous une semaine sans informatique ?	Définir un mode dégradé réaliste et l'éprouver.
Qui décide pendant la crise ?	Nommer un directeur de crise, un suppléant et un circuit d'arbitrage court.

PRINCIPE ZERVAL PRO

Une cartographie utile relie chaque mission à ses dépendances, à son responsable et à sa durée d'interruption tolérable.

SOCLE DE MAÎTRISE

Cinq fondamentaux à exiger

Ces mesures sont connues, peu spectaculaires et durablement efficaces. Leur constance compte davantage que l'accumulation de produits.

01	Authentification forte Activez le MFA sur la messagerie, les accès distants et les comptes d'administration. Privilégiez les mécanismes résistants à l'hameçonnage lorsque l'enjeu le justifie.
02	Sauvegardes isolées et testées Conservez au moins une copie hors d'atteinte de la production et testez réellement la restauration des données vitales.
03	Mises à jour maîtrisées Corrigez rapidement les services exposés et les outils critiques, avec validation et retour arrière préparé.
04	Journalisation exploitable Conservez les traces nécessaires pour détecter, comprendre et prouver. Attribuez leur consultation et leur durée de conservation.
05	Moindre privilège Séparez les usages courants et l'administration, retirez les droits inutiles et désactivez les comptes anciens.

DÉCISION DE DIRECTION

Cinq mesures suivies dans le temps valent mieux qu'un empilement de solutions mal gouvernées.

CONTINUITÉ ET DÉPENDANCES

Tenir lorsque le numérique s'arrête

Imaginez une semaine sans messagerie, facturation ni dossiers partagés. Un plan utile peut commencer sur une page : activités prioritaires, mode dégradé, responsables, contacts, ordre de reprise et critères de retour à la normale.

Un exercice court, mené avec la direction et le prestataire, révèle les numéros obsolètes, les décisions sans propriétaire et les dépendances oubliées. Le test donne sa valeur au plan.

> **À RETENIR**
> Le plan de continuité doit rester utilisable lorsque les procédures ordinaires et les outils habituels ne répondent plus.

Externaliser sans abandonner

Un prestataire prend en charge des opérations. La responsabilité de la mission reste dans l'organisation. Lorsqu'il traite des données personnelles, le contrat doit préciser l'alerte, la coopération, les journaux, les sauvegardes, les délais d'intervention, la conservation des preuves et la réversibilité.

Une attaque chez un sous-traitant peut déclencher des obligations pour plusieurs clients. Le responsable de traitement évalue le risque et procède aux notifications requises dans les délais. [S04]

RESPONSABILITÉS

Ce que le droit attend de la direction

Le cadre juridique fixe des obligations précises. Leur application dépend toujours du statut, du secteur, des données concernées et du contexte de l'incident.

RGPD

Toute violation de données personnelles est documentée. Lorsqu'elle présente un risque pour les droits et libertés des personnes, le responsable de traitement notifie la CNIL dans les meilleurs délais et, si possible, dans les 72 heures. Un risque élevé impose aussi d'informer les personnes concernées, sous réserve des exceptions prévues par les textes. [S04]

NIS 2

Pour les futures entités essentielles ou importantes, les organes de direction approuvent les mesures de gestion du risque, supervisent leur mise en œuvre et suivent une formation. La transposition française est toujours en cours à la date de cette édition. Depuis le 17 mars 2026, l'ANSSI met à disposition le Référentiel Cyber France, ReCyF, pour préparer les entités concernées. [S03]

> **POINT DE VIGILANCE**
> Le périmètre NIS 2 dépend notamment du secteur, de la taille, du statut et de critères spécifiques. Une TPE ou une PME ne relève pas automatiquement du dispositif.

PARTIE III

RÉAGIR

Dans les premières heures, préserver la mission, les faits et la capacité de décider.

PREMIÈRES DÉCISIONS

Stabiliser avant de réparer

La vitesse aide. La précipitation détruit des options. Éteindre, nettoyer ou réinstaller sans qualification préalable peut interrompre une activité vitale, effacer des traces et compliquer la reprise.

L'endiguement se décide au regard de la mission : isoler ce qui est touché, préserver les preuves et maintenir ce qui peut continuer sans aggraver l'incident. [S01][S06]

> **DÉCISION DE DIRECTION**
> Stabilisez avant de réparer. Nommez les faits avant d'adopter un récit. Réservez les actions irréversibles aux décisions explicitement justifiées.

Avant une action irréversible

Demandez ce que l'action protège, ce qu'elle risque de détruire, quelles traces elle efface et comment elle affecte les activités vitales. Cette discipline évite d'élargir une crise encore maîtrisable.

CONDUITE DE CRISE

La séquence des premières heures

Il s'agit d'une trame de décision. Chaque situation impose son propre rythme.

01	Activer Nommer le responsable de crise et ouvrir un journal des décisions.
02	Isoler Déconnecter les équipements touchés ou suspects sans couper à l'aveugle les systèmes indispensables.
03	Préserver Conserver les journaux, les messages, les supports et les horodatages. Suspendre le nettoyage précipité.
04	Qualifier Évaluer le périmètre, les missions atteintes, les données concernées et les accès compromis.
05	Alerter Mobiliser le prestataire, l'assureur, le conseil, le DPO et les autorités selon la situation.
06	Décider Arbitrer le mode dégradé, la communication, les notifications et l'ordre de reprise.

DÉCISIONS SENSIBLES

Rançon et notifications : décider avec méthode

Les décisions irréversibles se préparent avant l'incident et se prennent avec les compétences juridiques, techniques, humaines et financières nécessaires.

La ligne directrice française : ne pas payer

Cybermalveillance.gouv.fr recommande de ne pas payer. La restitution des données demeure incertaine et le paiement finance l'activité criminelle. Préservez les preuves, déposez plainte et faites-vous accompagner. [S05]

> **DÉCISION DE DIRECTION**
> Aucun dirigeant ne devrait arbitrer seul, sous la pression et sans mesurer les conséquences juridiques, humaines, financières et probatoires.

Notifier avec exactitude

Une attaque informatique ne déclenche pas automatiquement une notification à la CNIL. Il faut établir qu'une violation de données personnelles a eu lieu et apprécier le risque pour les personnes. Lorsque ce risque existe, une notification initiale intervient, si possible, dans les 72 heures. Elle peut être complétée au fil de l'investigation. Toute violation reste documentée. [S04]

D'autres signalements peuvent s'ajouter selon le statut de l'organisation. Déclenchez l'analyse juridique dès les premières heures, sans attendre la fin des investigations.

CONFIANCE

Communiquer avec précision

Une communication utile distingue quatre éléments : les faits établis, les inconnues, les actions engagées et la date du prochain point. Cette discipline protège davantage qu'une promesse rassurante que les faits pourraient démentir.

Protéger aussi les personnes

Une crise fatigue, désorganise et expose. Préparez les relais, limitez les horaires intenables, accompagnez les victimes et soutenez les équipes. La qualité des décisions dépend aussi de ces conditions de travail.

> **L'ESSENTIEL**
> Isolez de façon ciblée. Préservez avant de nettoyer. Qualifiez avant d'affirmer. Notifiez selon le risque. Communiquez avec exactitude. Reconstruisez depuis des sources saines.

IV

PARTIE IV

ÉPROUVER ET AGIR

Confronter la doctrine aux faits, puis engager les décisions utiles.

CAS PUBLIC

Corbeil-Essonnes : quand la mission doit tenir

Dans la nuit du 20 au 21 août 2022, le Centre hospitalier Sud-Francilien subit un rançongiciel. Une rançon de 10 millions d'euros est réclamée. Le système est paralysé, des patients sont orientés vers d'autres établissements et l'hôpital fonctionne en mode dégradé. [S08]

L'enseignement pour un dirigeant

La continuité de la mission se prépare avant la crise. Le refus de payer suit la doctrine publique française. Le cas rappelle surtout l'importance du mode dégradé, de l'arbitrage, de la coordination et d'une reconstruction propre.

> **LEÇON**
> La résilience se mesure à la capacité de poursuivre la mission, de décider et de reconstruire malgré la crise.

Ce que montre le panorama 2025

L'ANSSI a eu connaissance de 1 366 incidents confirmés en 2025. L'éducation et la recherche, les ministères et collectivités territoriales, la santé et les télécommunications concentrent 76 % de ces incidents. Les PME, TPE et ETI restent la catégorie la plus représentée parmi les victimes de rançongiciel observées. [S01]

Ces données correspondent au périmètre de l'Agence. Elles rappellent qu'une petite structure ne peut compter sur sa discrétion lorsque ses accès visibles et ses dépendances restent mal maîtrisés.

MÉMENTO

Dix actions à engager cette semaine

Passez cette liste en revue avec votre direction et votre prestataire. Attribuez un responsable et une échéance à chaque action retenue.

01	MFA Protéger la messagerie, les accès distants et l'administration par une authentification multifacteur.
02	Sauvegardes Isoler au moins une copie et tester la restauration des données vitales.
03	Mises à jour Définir qui corrige quoi, dans quel délai et avec quelle preuve.
04	Droits Séparer les comptes courants et administrateurs, puis retirer les accès inutiles.
05	Traces Activer les journaux utiles, les centraliser si possible et fixer leur durée de conservation.
06	Équipes Entraîner les équipes à vérifier les demandes inhabituelles, notamment les changements de coordonnées bancaires.
07	Prestataire Écrire les rôles, les délais, la coopération attendue et les modalités de conservation des preuves.
08	Crise Rédiger une fiche d'une page : qui décide, qui appelle, quelles activités maintenir et dans quel ordre reprendre.
09	Rançon Formaliser à froid la ligne de non-paiement et le circuit d'arbitrage.
10	Contacts Conserver hors ligne les coordonnées du prestataire, de l'assureur, du DPO, des autorités et du conseil.

PREMIÈRES 72 HEURES

Une carte de décision, pas un chronomètre

Les plages horaires donnent un ordre de travail. Elles s'adaptent à la gravité, au périmètre et aux obligations propres à chaque organisation.

01	0 à 2 h : stabiliser Activer la cellule, isoler de façon ciblée, préserver les traces et maintenir les missions possibles.
02	2 à 8 h : qualifier Évaluer les accès compromis, les données concernées, l'impact métier, les dépendances et les premières hypothèses.
03	8 à 24 h : décider Arbitrer le mode dégradé, la reprise, la communication, les autorités, l'assureur et la stratégie probatoire.
04	24 à 72 h : notifier Notifier la CNIL lorsqu'une violation présente un risque. Informer les personnes si ce risque est élevé.
05	Après : reconstruire Restaurer depuis des sources saines, corriger la cause, contrôler les accès et organiser le retour d'expérience.

Trois questions à poser au prestataire

01	Sauvegardes Où se trouvent-elles, sont-elles isolées et quand la dernière restauration a-t-elle été testée ?
02	Décision Qui agit, dans quel délai, et qui autorise une coupure, un nettoyage ou une restauration ?
03	Preuves Comment les journaux et les preuves sont-ils conservés et restitués en cas d'incident ?

REPÈRES DE DIRECTION

Sept critères pour décider

Gardez ces critères comme une grille d'arbitrage. Ils servent à questionner une décision, un prestataire ou un plan de crise.

01	Mission La cybersécurité protège d'abord la mission de l'organisation.
02	Faits Une décision solide distingue les faits, les hypothèses et les inconnues.
03	Responsabilité L'externalisation transfère des opérations, jamais la responsabilité de la mission.
04	Capacité Une sauvegarde jamais restaurée reste une promesse.
05	Irréversibilité Une action irréversible se justifie par ce qu'elle protège et ce qu'elle détruit.
06	Confiance Une communication exacte, sobre et régulière protège la relation.
07	Direction Le dirigeant décide malgré l'incertitude et garde la maîtrise de l'arbitrage.

Zerval PRO, aux côtés des dirigeants

Zerval PRO transforme les signaux techniques en décisions compréhensibles : gouvernance du risque, préparation à la crise, investigation des faits, remédiation et preuve. Ce livret ouvre le travail. Il permet d'examiner vos missions, vos dépendances et votre capacité à tenir.

GOUVERNER. RÉAGIR. PROUVER.

pro.zerval.io • contact@zerval.io

MÉTHODE

Sources et références

Références officielles et primaires utilisées pour les chiffres, les obligations et les recommandations. Vérification éditoriale : 24 août 2026.

[S01]	ANSSI / CERT-FR, Panorama de la cybermenace 2025, publié le 11 mars 2026. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf
[S02]	ENISA, ENISA Threat Landscape 2025, version 1.2, 9 janvier 2026. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
[S03]	ANSSI, Directive NIS 2 et Référentiel Cyber France : état de la transposition. https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/
[S04]	CNIL, Notifier une violation de données personnelles. https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles
[S05]	Cybermalveillance.gouv.fr, Rançongiciel : isoler, alerter, préserver les preuves et ne pas payer. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares
[S06]	CERT-FR, Fiche réflexe : chiffrement ou effacement en cours. https://cert.ssi.gouv.fr/uploads/CERTFR-2024-RFX-001-2.pdf
[S07]	ANSSI, Guide d'hygiène informatique. https://messervices.cyber.gouv.fr/documents-guides/guide_hygiene_informatique_anssi.pdf
[S08]	Sénat, Éléments publics sur la cyberattaque du Centre hospitalier Sud-Francilien. https://www.senat.fr/rap/a22-117-9/a22-117-90.html

NOTE ÉDITORIALE

Les chiffres décrivent les périmètres observés par les organismes cités. Les obligations dépendent du statut, du secteur et du contexte de chaque organisation.

VOIR CLAIR.
AGIR JUSTE.
TENIR.

La direction garde la maîtrise lorsque les faits sont qualifiés,
les décisions assumées et les traces conservées.