ZERVAL
PRO

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

STATUT : ÉDITION PUBLIQUE • VERSION 1.0 • AOÛT 2026

CODEX — Édition Dirigeants

Une version condensée de la doctrine Zerval PRO pour décider sans devenir expert.

PROMESSE DE LECTURE

En vingt minutes : comprendre ce qui est réellement en jeu, décider avant la crise et conserver la maîtrise dans les premières heures.

Portée

Ce livret s'adresse aux dirigeants de TPE, PME, collectivités, associations et cabinets. Il ne remplace ni un audit, ni une analyse de risque propre à votre organisation, ni un avis juridique. Les données et cadres réglementaires sont vérifiés à la date du 11 août 2026.

Édition

Publié sous la marque Zerval PRO — Lyon, France — contact@zerval.io — pro.zerval.io.

Ce que vous devez retenir

QUESTION DE DIRECTION	DÉCISION ATTENDUE
Qu'est-ce qui ne doit jamais s'arrêter ?	Identifier trois à cinq missions vitales et leur durée d'interruption tolérable.
Quelles données ne doivent jamais fuiter ?	Classer les informations critiques et limiter strictement les accès.
Que se passe-t-il si le prestataire est indisponible ?	Prévoir rôles, délais, réversibilité, sauvegardes et contacts d'escalade dans le contrat.
Comment travaillons-nous une semaine sans informatique ?	Définir un mode dégradé réaliste et le tester.
Qui décide le jour de la crise ?	Nommer un directeur de crise, un suppléant et un circuit de décision court.

Comment lire ce livret

LECTURE 01 — 5 MINUTES
Lisez les ouvertures de parties, les encadrés « Décision de direction » et le mémento final.

LECTURE 02 — 20 MINUTES
Suivez l'ordre : comprendre, gouverner, réagir, puis confronter les repères à votre organisation.

LECTURE 03 — EN COMITÉ DE DIRECTION
Utilisez les tableaux comme ordre du jour : missions vitales, dépendances, crise, notification et responsabilité.

Sommaire

ZERVAL PRO

PARTIE I

COMPRENDRE

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

La cybersécurité est une décision

Vous n'avez pas besoin de devenir expert

Vous avez besoin de savoir ce qui est vital, ce que vous acceptez de risquer et ce que vous refusez de perdre. Un logiciel ne répondra jamais à ces questions. Elles relèvent de la direction.

La maturité ne se mesure donc pas au nombre de produits achetés, mais à la qualité des arbitrages : priorités explicites, responsabilités nommées, dépendances connues et décisions documentées.

DÉCISION DE DIRECTION

Traitez la cybersécurité comme un sujet de continuité, de confiance et de responsabilité — pas comme une ligne d'achat informatique.

Ce que vous protégez réellement

Un incident n'abîme pas d'abord des machines. Il affecte la promesse faite aux clients, la capacité à facturer ou produire, la confidentialité des dossiers, la paie, les services rendus et la confiance des équipes. Les systèmes ne sont que les moyens de cette mission.

Protéger l'organisation, c'est préserver sa capacité à poursuivre sa mission malgré l'incertitude. Cette formulation change l'ordre des priorités : on part de l'activité essentielle, puis on remonte vers les données, les applications, les prestataires et les équipements qui la rendent possible.

La menace réelle, sans dramatisation

3 586 événements traités par l'ANSSI en 2025	**1 366** incidents confirmés portés à sa connaissance
128 compromissions par rançongiciel recensées	**60 %** des accès initiaux observés par l'ENISA passent par l'hameçonnage

Les chiffres ne décrivent pas toute la menace : ils reflètent les incidents connus des autorités et leurs périmètres d'observation. Ils suffisent néanmoins à établir trois faits. L'hameçonnage demeure un accès initial majeur ; le rançongiciel reste la menace jugée la plus impactante en Europe ; et les PME, TPE et ETI restent la catégorie la plus représentée parmi les victimes de rançongiciels observées par l'ANSSI. [S01][S02]

Pourquoi les petites structures sont exposées

La plupart des attaques opportunistes ne recherchent pas une entreprise prestigieuse. Elles recherchent une surface visible, un accès faible, un mot de passe réutilisé, un service non corrigé ou un fournisseur compromis. La taille ne protège pas ; l'accessibilité décide souvent de la cible.

En 2025, l'ANSSI indique que les PME, TPE et ETI restent la catégorie la plus affectée par les rançongiciels. Les attaques peuvent interrompre la production ou le service pendant plusieurs semaines, alors même que les moyens de réponse sont plus limités. [S01]

Regarder le risque, pas chercher le risque zéro

Le risque zéro n'existe pas. La bonne gouvernance consiste à identifier les scénarios qui peuvent réellement compromettre la mission, à réduire les plus graves, à transférer certains risques et à accepter le reste en connaissance de cause. Un risque accepté doit avoir un propriétaire, une justification et une date de réexamen.

> **PRINCIPE ZERVAL PRO**
> La mission du dirigeant n'est pas d'éliminer le risque. Elle est de prendre des décisions proportionnées, documentées et assumées malgré l'incertitude.

Trois questions immédiates

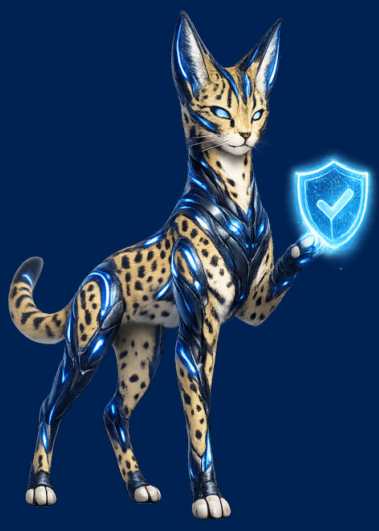
1	**Mission** Quelles activités doivent continuer même si les systèmes sont indisponibles ?
2	**Confiance** Quelles données ou décisions ne peuvent être exposées sans dommage durable ?
3	**Tolérance** Combien de temps l'organisation peut-elle fonctionner en mode dégradé ?

ZERVAL PRO

PARTIE II

GOUVERNER

Les décisions les moins coûteuses se prennent avant la crise, à froid.



Partir des missions, pas des outils

La première question n'est pas « quel logiciel installer ? », mais « qu'est-ce qui ne doit jamais s'arrêter ou fuiter ? ». Identifiez trois à cinq missions vitales, puis les personnes, données, fournisseurs et systèmes dont elles dépendent.

QUESTION DE DIRECTION	DÉCISION ATTENDUE
Qu'est-ce qui ne doit jamais s'arrêter ?	Identifier trois à cinq missions vitales et leur durée d'interruption tolérable.
Quelles données ne doivent jamais fuiter ?	Classer les informations critiques et limiter strictement les accès.
Que se passe-t-il si le prestataire est indisponible ?	Prévoir rôles, délais, réversibilité, sauvegardes et contacts d'escalade dans le contrat.
Comment travaillons-nous une semaine sans informatique ?	Définir un mode dégradé réaliste et le tester.
Qui décide le jour de la crise ?	Nommer un directeur de crise, un suppléant et un circuit de décision court.

Les fondamentaux à exiger

1. **Authentification forte**
   Activez le MFA sur la messagerie, les accès distants et les comptes d'administration. Préférez les mécanismes résistants à l'hameçonnage lorsque l'enjeu le justifie.
2. **Sauvegardes isolées et testées**
   Une copie restée accessible au réseau peut être chiffrée avec la production. Testez la restauration sur les données réellement vitales.
3. **Mises à jour maîtrisées**
   Corrigez rapidement les services exposés et les outils critiques, avec une procédure de validation et de retour arrière.
4. **Journalisation exploitable**
   Conservez les traces nécessaires pour détecter, comprendre et prouver. Définissez qui les consulte et combien de temps elles sont gardées.
5. **Moindre privilège**
   Séparez les comptes usuels et administrateurs ; retirez les droits inutiles et désactivez les comptes anciens.

DÉCISION DE DIRECTION

Cinq mesures constantes valent mieux qu'un empilement de produits non gouvernés.

Continuité : tenir lorsque le numérique s'arrête

Que faites-vous si, demain matin, la messagerie, la facturation ou les dossiers partagés sont indisponibles pendant une semaine ? Un plan utile tient d'abord en une page : activités prioritaires, mode dégradé, responsables, contacts, ordre de reprise et critères de retour à la normale.

Le plan ne vaut que s'il est testé. Un exercice court, mené avec la direction et le prestataire, révèle les numéros obsolètes, les décisions non attribuées et les dépendances oubliées.

> **PRINCIPE ZERVAL PRO**
> Le véritable plan de continuité n'est pas celui qui est écrit. C'est celui qui fonctionne lorsque les procédures habituelles cessent de fonctionner.

Prestataire et cloud : externaliser sans abandonner

L'externalisation transfère des opérations, jamais la responsabilité de la mission ni, pour les données personnelles, les obligations du responsable de traitement. Le contrat doit préciser l'alerte, la coopération, la conservation des preuves, la disponibilité des journaux, la localisation et l'isolement des sauvegardes, les délais d'intervention et la réversibilité.

Une cyberattaque chez un sous-traitant peut déclencher des obligations pour plusieurs organisations. La CNIL rappelle en 2026 que le responsable de traitement reste tenu d'évaluer le risque et, si nécessaire, de notifier dans les délais. [S04]

Ce que le droit attend réellement

RGPD. Toute violation doit être documentée. La notification à la CNIL intervient dans les meilleurs délais et, si possible, sous 72 heures lorsqu'elle est susceptible d'engendrer un risque pour les droits et libertés des personnes. Si le risque est élevé, les personnes concernées doivent aussi être informées, sauf cas particuliers. [S04]

NIS 2. Pour les entités essentielles ou importantes, les organes de direction doivent approuver les mesures de gestion du risque, en superviser la mise en œuvre et suivre une formation. En France, la transposition nationale demeure en cours à la date d'édition ; l'ANSSI a publié en mars 2026 le Référentiel Cyber France pour préparer les futures entités concernées. [S03]

> **POINT DE VIGILANCE**
> NIS 2 ne s'applique pas indistinctement à toutes les TPE et PME. Le secteur, la taille, le statut et certains critères spécifiques déterminent le périmètre.

ZERVAL PRO

PARTIE III

III

RÉAGIR

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

Qualifier sans détruire

La première erreur consiste à confondre vitesse et précipitation. Tout éteindre ou tout réinstaller peut interrompre des activités essentielles, effacer des traces et compliquer la reprise. L'ANSSI rappelle que les mesures d'endiguement doivent être arbitrées : isoler ce qui est touché, préserver les preuves et maintenir ce qui peut fonctionner sans aggraver l'incident. [S01][S06]

DÉCISION DE DIRECTION

Stabiliser avant de réparer. Nommer les faits avant d'adopter un récit. Réserver les actions irréversibles aux décisions explicitement justifiées.

La séquence des premières heures

1	**Activer** Nommer un responsable de crise et ouvrir un journal des décisions.
2	**Isoler** Déconnecter les équipements touchés ou suspects sans couper à l'aveugle les systèmes indispensables.
3	**Préserver** Conserver journaux, messages, supports et horodatages ; éviter le nettoyage précipité.
4	**Qualifier** Évaluer le périmètre, l'impact sur les missions, les données concernées et les accès compromis.
5	**Alerter** Mobiliser prestataire, assureur, conseil, DPO et autorités selon la situation.
6	**Décider** Arbitrer communication, mode dégradé, notification et ordre de reprise.

Rançon : la ligne directrice est de ne pas payer

Cybermalveillance.gouv.fr recommande de ne pas payer : aucune restitution n'est garantie et le paiement finance l'activité criminelle. L'organisation doit préserver les preuves, déposer plainte et se faire accompagner. [S05]

Cette ligne directrice doit être intégrée au plan de crise avant l'incident. Les échanges éventuels avec un attaquant, la temporisation ou la recherche d'informations ne doivent jamais être confondus avec une garantie de récupération ni avec un transfert de décision hors de la direction.

> **PRINCIPE ZERVAL PRO**
> Une décision irréversible ne se prend ni seul, ni sous la pression, ni sans examiner ses conséquences juridiques, humaines, financières et probatoires.

Notifier avec exactitude

Une cyberattaque n'entraîne pas automatiquement une notification à la CNIL. Il faut établir l'existence d'une violation de données personnelles et apprécier le risque. Lorsqu'un risque existe, la notification intervient au plus tard dans les 72 heures si possible ; elle peut être complétée ensuite. Toute violation doit rester documentée. [S04]

Selon le statut de l'organisation, d'autres notifications ou signalements peuvent s'ajouter. Le bon réflexe consiste à déclencher immédiatement l'analyse juridique plutôt qu'à attendre la fin de l'investigation.

Communiquer pour protéger la confiance

Dire ce qui est établi, ce qui reste inconnu, ce qui est fait et quand un nouveau point sera communiqué. Une information sobre et cohérente vaut mieux qu'une promesse rassurante que les faits démentiront.

L'humain d'abord

Une crise fatigue, désorganise et expose les personnes. Prévoir les relais, limiter les horaires impossibles, protéger les victimes et soutenir les équipes n'est pas accessoire : c'est une condition de la continuité et de la qualité des décisions.

> **L'ESSENTIEL**
> Isoler sans tout couper. Préserver avant de nettoyer. Qualifier avant d'affirmer. Notifier selon le risque. Communiquer avec exactitude. Reconstruire depuis des sources saines.

ZERVAL PRO

IV

PARTIE IV

ÉPROUVER & AGIR

Des faits publics, un mémento et des questions à poser dès cette semaine.

Corbeil-Essonnes : la mission avant les systèmes

Dans la nuit du 20 au 21 août 2022, le Centre hospitalier Sud-Francilien est frappé par un rançongiciel. Une rançon de 10 millions est réclamée. Le système est paralysé, des patients sont orientés vers d'autres établissements et l'hôpital fonctionne en mode dégradé. Les coûts publics évoqués portent sur la réponse et la reconstruction, indépendamment de la rançon. [S08]

Ce que le dirigeant doit en retenir. La continuité de la mission se prépare avant la crise. Le refus de payer est cohérent avec la doctrine publique française, mais l'issue observée ne permet pas d'affirmer ce qu'un autre choix aurait produit. L'enseignement solide est ailleurs : mode dégradé, arbitrage, coordination et reconstruction sont des capacités de gouvernance.

> **LEÇON**
> Une organisation résiliente n'est pas celle qui évite toute crise. C'est celle qui conserve assez de maîtrise pour continuer à servir et reconstruire proprement.

Ce que montre le panorama 2025

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

Ces données ne signifient pas que tous les secteurs sont exposés de la même manière. Elles rappellent qu'une petite structure ne peut pas compter sur sa discrétion : les attaques opportunistes frappent les accès visibles et les dépendances mal maîtrisées.

Mémento — agir dès cette semaine

Dix actions à confronter à votre direction et à votre prestataire.

1	**MFA** Activer l'authentification multifacteur sur la messagerie, les accès distants et l'administration.
2	**Sauvegardes** Isoler au moins une copie et tester réellement la restauration des données vitales.
3	**Mises à jour** Définir qui corrige quoi, dans quel délai, avec quelle preuve de réalisation.
4	**Droits** Séparer les comptes usuels et administrateurs ; retirer les accès inutiles.
5	**Traces** Activer les journaux utiles, les centraliser si possible et définir leur durée de conservation.
6	**Équipes** Entraîner à vérifier les demandes inhabituelles, notamment les changements de coordonnées bancaires.
7	**Prestataire** Écrire les rôles, délais, obligations de coopération et modalités de conservation des preuves.
8	**Crise** Rédiger une fiche d'une page : qui décide, qui appelle, quelles activités maintenir, dans quel ordre reprendre.
9	**Rançon** Formaliser à froid la ligne directrice 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.

La carte des premières 72 heures

Une séquence de décision, pas une chronologie rigide.

1	**0–2 h | Stabiliser** Activer la cellule, isoler de façon ciblée, préserver les traces, maintenir les missions possibles.
2	**2–8 h | Qualifier** Périmètre, accès compromis, données concernées, impact métier, dépendances et premières hypothèses.
3	**8–24 h | Décider** Mode dégradé, priorités de reprise, communication, autorités, assureur et stratégie probatoire.
4	**24–72 h | Notifier** Si une violation de données présente un risque : notification CNIL ; information des personnes si le risque est élevé. Compléter ensuite si nécessaire.
5	**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

1
Où sont nos sauvegardes, sont-elles réellement isolées et quand la dernière restauration a-t-elle été testée ?

2
Qui fait quoi, dans quel délai, et qui peut décider d'une coupure, d'un nettoyage ou d'une restauration ?

3
Comment conservez-vous les journaux et les preuves, et comment nous les restituez-vous en cas d'incident ?

Repères Zerval PRO pour décider

À garder en tête comme des critères d'arbitrage, non comme des slogans.

PRINCIPE 01
La cybersécurité protège la mission avant de protéger les machines.

PRINCIPE 02
La qualité d'une décision dépend de la distinction entre faits, hypothèses et inconnues.

PRINCIPE 03
L'externalisation transfère des opérations ; elle ne transfère pas la responsabilité de la mission.

PRINCIPE 04
Une sauvegarde qui n'a jamais été restaurée reste une promesse, pas une capacité.

PRINCIPE 05
Une action irréversible doit être justifiée par ce qu'elle protège et ce qu'elle détruit.

PRINCIPE 06
La communication de crise protège la confiance lorsqu'elle est exacte, sobre et régulière.

PRINCIPE 07
La mission du dirigeant est de décider malgré l'incertitude, pas de prétendre la supprimer.

Zerval PRO, aux côtés des dirigeants

Zerval PRO transforme les enjeux techniques en décisions compréhensibles : gouvernance du risque, préparation à la crise, investigation des faits, remédiation et accompagnement. Ce livret n'est pas une fin ; il est un point de départ pour examiner vos missions, vos dépendances et votre capacité à tenir.

pro.zerval.io • contact@zerval.io

Sources & méthode

Références officielles et primaires utilisées pour vérifier les chiffres, les obligations et les recommandations. Les liens sont cliquables.

[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 et préparation des entités.
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 ; règles relatives au délai de 72 heures.
https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles

[S05] **Cybermalveillance.gouv.fr**
Rançongiciels : isoler, alerter, ne pas payer, préserver les preuves et déposer plainte.
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

[S06] **CERT-FR**
Fiche réflexe : chiffrement ou effacement en cours — qualification.
https://cert.ssi.gouv.fr/uploads/CERTFR-2024-RFX-001-2.pdf

[S07] **ANSSI**
Guide d'hygiène informatique — mesures de sécurité essentielles.
https://messervices.cyber.gouv.fr/documents-guides/guide_hygiene_informatique_anssi.pdf

[S08] **Sénat**
Éléments publics sur la cyberattaque du Centre hospitalier Sud-Francilien et ses conséquences.
https://www.senat.fr/rap/a22-117-9/a22-117-90.html

NOTE ÉDITORIALE

Les chiffres décrivent les périmètres observés par les organismes cités ; ils ne mesurent pas l'ensemble des incidents en France ou en Europe. Les obligations dépendent du statut, du secteur et du contexte de chaque organisation.