Sécuriser son Entreprise — Édition 2027

Protéger le capital physique, intellectuel et industriel

Gouvernance & Sûreté

Analyse des Risques

Cybersécurité

Conformité 2027

GUIDE ADESS — ÉDITION 2027

Introduction — Un environnement de menaces radicalement transformé

Contexte 2027

Conflits de haute intensité en Europe, cyberguerre hybride, espionnage industriel massif par IA, montée du crime organisé transnational. Entre 2020 et 2025, le nombre de cyberattaques a doublé. En 2025, **1 366 incidents** ont été portés à la connaissance de l'ANSSI (1 361 en 2024).

Nouvelles menaces émergentes

- Attaques par IA générative : deepfakes, phishing ultra-ciblé
- Sabotage de chaînes d'approvisionnement
- Menaces sur les infrastructures critiques (OT/IoT)
- Cibles élargies : TPE, PME et collectivités désormais aussi visées que les grands groupes

Objectif du guide

Conseiller les organisations dans la protection de leur patrimoine humain, matériel et immatériel — mis à jour pour intégrer l'ensemble des réglementations 2023-2027 : NIS2, AI Act, DORA, PST 2026-2030, Passeport de prévention, CSRD.

PARTIE 1

Gouvernance & Politique Sécurité-Sûreté

Organisation, responsabilités et cadre stratégique de la sécurité globale d'entreprise.

Les Grandes Fonctions de l'Entreprise et la Sécurité

Direction Générale

Politique sécurité, obligation de résultat

DRH

Formation, passeport de prévention

DAF

Assurances, financement sécurité

RSSI

Cybersécurité, NIS2 (obligatoire)

Direction Production

Protection process, secrets industriels

Services Généraux

Accueil, contrôle d'accès

Direction Générale

Politique de sécurité-sûreté, obligation de sécurité et de résultat (Art. L4121-1 Code du travail).

DRH

Programme de formation SST, règlement intérieur, **passeport de prévention obligatoire depuis 2026**.

DAF

Assistance juridique, dossiers assurance, financement des investissements sécurité-sûreté.

Direction Production

Protection du process contre la malveillance, secrets de fabrication, prototypes.

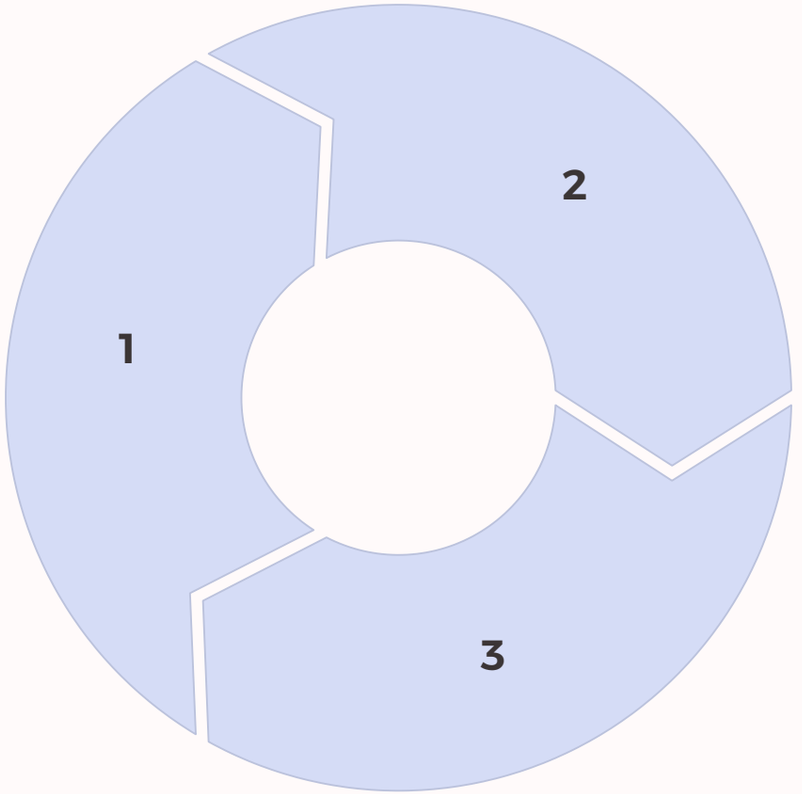
Services Généraux

Accueil, contrôle d'accès, lien avec la prévention situationnelle.

RSSI — Nouveauté 2027

Intégration d'un Responsable Sécurité des Systèmes d'Information **obligatoire pour les entités NIS2**.

Mener une Politique Sécurité-Sûreté Globale



1 Sécurité Physique

Protection des locaux, contrôle d'accès, vidéosurveillance

2 Cybersécurité

Protection SI, NIS2, ISO 27001

3 Continuité d'Activité

PCA, PRA, gestion de crise

Approche intégrée 2027

Sécurité physique + cybersécurité + sûreté + continuité d'activité — **les silos sont obsolètes**. La politique globale articule : règlement intérieur, registre de sécurité, SOP, consignes incendie, charte informatique, RGPD, propriété industrielle (INPI).

Obligation de résultat

L'employeur est responsable pénalement et civilement en cas de manquement (Art. L4121-1 à L4121-5 Code du travail).

Démarche d'audit — 4 étapes

1. Préparation
2. Étude de l'existant
3. Analyse organisationnelle
4. Recommandations et plan d'action

Indicateurs de performance

Taux d'incidents, délais de détection/réponse (MTTD, MTTR), taux de conformité réglementaire, résultats des exercices de crise.

Sauvegarde du Patrimoine — Humain, Matériel, Immatériel

Patrimoine Humain

Sécurité physique des collaborateurs, formation, gestion des RPS

Patrimoine Matériel

Locaux, équipements, véhicules, stocks

Patrimoine Immatériel

Données, brevets, savoir-faire, modèles IA

Patrimoine Humain

Sécurité physique des collaborateurs, formation, sensibilisation, gestion des risques psychosociaux (RPS) — renforcée par le **PST 2026-2030** (lancé le 5 juin 2026).

Patrimoine Matériel

Locaux, équipements, véhicules, stocks — protection physique, maintenance préventive, couverture assurance adaptée.

Patrimoine Immatériel

Données clients, brevets, savoir-faire, marques, logiciels — double protection juridique (INPI, secret des affaires) et technique (DLP, chiffrement).

Nouveauté 2027 — Actifs IA

Les modèles entraînés et données d'entraînement constituent un **nouveau patrimoine immatériel** à protéger — secret des affaires, AI Act, RGPD.

PARTIE 2

Analyse et Prévention des Risques

Identifier, évaluer, traiter et surveiller les risques pour construire une organisation résiliente.

Concepts Fondamentaux : Risque, Menace, Vulnérabilité

Risque

Probabilité qu'une menace exploite une vulnérabilité et génère un impact négatif

Menace

Événement potentiel susceptible de causer un dommage

Vulnérabilité

Faiblesse d'un actif pouvant être exploitée

Impact

Conséquences financières, opérationnelles, réputationnelles

Risque

Probabilité qu'une menace exploite une vulnérabilité et génère un impact négatif sur l'organisation.

Menace

Événement potentiel (malveillant ou accidentel) susceptible de causer un dommage.

Vulnérabilité

Faiblesse d'un actif ou d'un contrôle pouvant être exploitée par un attaquant.

Impact

Conséquences financières, opérationnelles, réputationnelles, juridiques.

Nouvelles menaces 2027

Attaques par IA générative, deepfakes de dirigeants, data poisoning, attaques OT/IoT industriels.

Diagramme de Ishikawa (5M) : Milieu, Main-d'œuvre, Méthodes, Matériels, Matières — outil d'analyse des causes racines appliqué à la sécurité.

Prévenir les Risques en Entreprise

1. Inventorier

Cartographier tous les actifs à protéger

2. Valoriser

Évaluer l'importance de chaque actif

3. Définir les parades

Choisir les mesures de protection adaptées

4. Identifier les points critiques

Prioriser les risques majeurs

5. Réviser

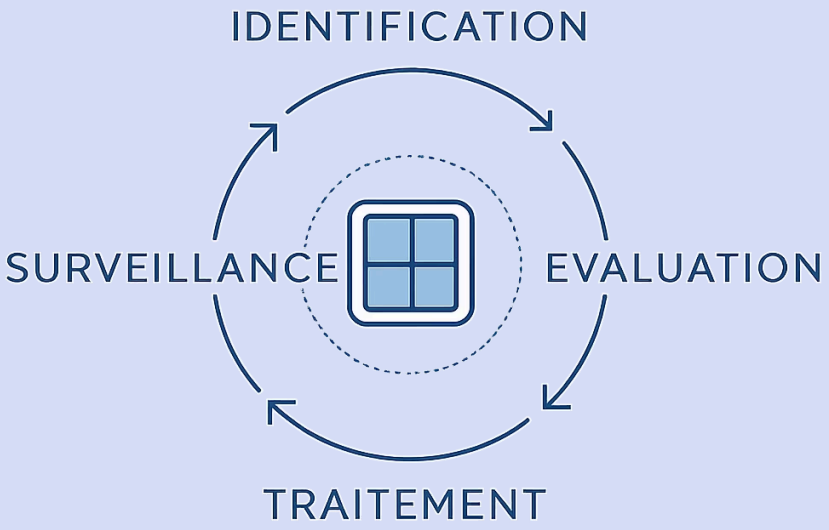
Mettre à jour régulièrement la table des risques

9 principes généraux de prévention (Code du travail)

1. Éviter les risques
2. Évaluer ceux qui ne peuvent être évités
3. Combattre les risques à la source
4. Adapter le travail à l'homme
5. Tenir compte de l'évolution de la technique
6. Remplacer le dangereux par le non ou moins dangereux
7. Planifier la prévention
8. Prendre des mesures collectives en priorité
9. Donner des instructions appropriées aux travailleurs

Méthode EBIOS Risk Manager

Référentiel ANSSI recommandé pour l'analyse de risques cyber — mis à jour en 2024. Gestion des risques en 5 étapes : inventorier → valoriser → définir les parades → identifier les points critiques → réviser la table des risques.



Processus de Management des Risques

1

1. Identification

Cartographie des actifs, des menaces et des scénarios de risque.

2

2. Évaluation

Cotation probabilité × impact, matrice de criticité.

3

3. Traitement

Accepter, réduire, transférer (assurance) ou éviter le risque.

4

4. Monitoring

Tableau de bord des risques, revue périodique, reporting à la direction.

Normes de référence 2027

- **ISO 31000** — management des risques
- **ISO 27005** — risques systèmes d'information
- **ISO 22301** — continuité d'activité

Intégration ESG — CSRD

Les risques sécurité-sûreté s'intègrent désormais dans les rapports de durabilité (Corporate Sustainability Reporting Directive, applicable depuis 2024-2025).

PARTIE 3

Gestion de Crise et Continuité d'Activité

Anticiper, planifier et répondre aux crises pour préserver la résilience organisationnelle.

Comprendre la Crise en Entreprise

Écrans d'Alerte

Surveillance en temps réel des indicateurs de crise

Données en Temps Réel

Flux d'information pour la prise de décision

Cellule de Crise

Équipe dédiée à la gestion de l'incident

Coordinateur

Pilotage et arbitrage des actions

Définition

Événement soudain ou progressif qui dépasse les capacités de réponse ordinaires de l'organisation et menace ses intérêts vitaux.

7 dimensions d'une crise

- Médiatique
- Juridique
- Humaine et sociale
- Technique
- Éthique
- Politique et institutionnelle
- Économique

7 parties prenantes

- Salariés
- Fournisseurs
- État et collectivités
- Financiers
- Propriétaires/actionnaires
- Clients
- Médias

Nouvelles crises 2027

- Cyberattaque par rançongiciel avec exfiltration de données
- Crise de réputation par deepfake
- Rupture de chaîne d'approvisionnement critique
- Crise climatique extrême (inondations, canicules)

Typologies de Crises

Externe / Technique-Économique

Boycott, mauvaise performance, fermeture de sites.

Externe / Social-Humain

Accident industriel, panne informatique, défectuosité produit.

Interne / Technique-Économique

Sabotage, chantage, fraude, rumeur.

Interne / Social-Humain

Conflit social, sabotage interne, fuite d'informations.

Externe / Technique-Économique

Boycott produit, mauvaise performance économique, produit de substitution, fermeture de sites.

Externe / Social-Humain

Accident industriel, panne informatique, défectuosité produit, dysfonctionnement de gouvernance.

Interne / Technique-Économique

Terrorisme, sabotage, chantage, émeute civile, fraude, rumeur.

Interne / Social-Humain

Conflit social, disparition d'hommes clés, sabotage interne, fraude, fuite d'informations confidentielles.

Ajout 2027 : crise cyber (ransomware, violation de données RGPD), crise IA (biais algorithmique, décision automatisée contestée), crise climatique extrême.

Le Plan de Gestion de Crise

Analyse des Risques

Identification des scénarios de crise potentiels

Procédure de Réponse

Actions à mener selon le type de crise

Activation

Déclenchement de la cellule de crise

Communication

Stratégie interne et externe, porte-parole

Contacts d'Urgence

Annuaire des parties prenantes clés

Bilan

Retour d'expérience post-crise

6 composantes du plan

1. Analyse des risques
2. Procédure de réponse
3. Protocole d'activation
4. Stratégie de communication
5. Contacts d'urgence
6. Bilan d'après-crise

6 étapes d'élaboration

1. Former une équipe
2. Définir les scénarios
3. Rédiger les procédures
4. Tester (exercices)
5. Former les acteurs
6. Réviser régulièrement

Obligation NIS2 — Notification d'incidents

Les entités essentielles et importantes doivent disposer d'un plan de réponse aux incidents cyber avec notification à l'ANSSI :

- **24h** — alerte précoce
- **72h** — notification complète
- **1 mois** — rapport final

Amendes jusqu'à **10 M€ ou 2%** du chiffre d'affaires mondial pour une entité essentielle.

PCA / PRA

Plan de Continuité et Plan de Reprise d'Activité — obligatoires pour les secteurs critiques (NIS2, DORA pour le secteur financier).

La Cellule de Crise

Directeur de Crise
Décision et arbitrage final

Communication
Gestion des messages internes et externes

Juridique
Conseil légal et gestion des responsabilités

Technique IT
Réponse aux incidents cyber et systèmes

Ressources Humaines
Gestion du personnel et soutien

Référent Sûreté
Interface avec les forces de l'ordre



Directeur de crise
DG ou mandataire — décision, arbitrage, interface avec les autorités.



Responsable communication
Communication interne/externe, gestion des réseaux sociaux, porte-parole désigné.



Responsable juridique
Conseil légal, gestion des obligations de notification réglementaires.



Responsable technique/IT
Coordination opérationnelle, gestion des systèmes, réponse aux incidents cyber.



Responsable RH & Sûreté
Gestion du personnel, referent sûreté, coordination avec les forces de l'ordre.

Outils 2027

Plateforme de gestion de crise collaborative (ex. Everbridge, Crises Control), communication chiffrée, salle de crise virtuelle. Exercices de simulation annuels obligatoires pour les OIV et entités NIS2.

La Gestion de Crise en 7 Étapes

1. Analyser et Prévenir

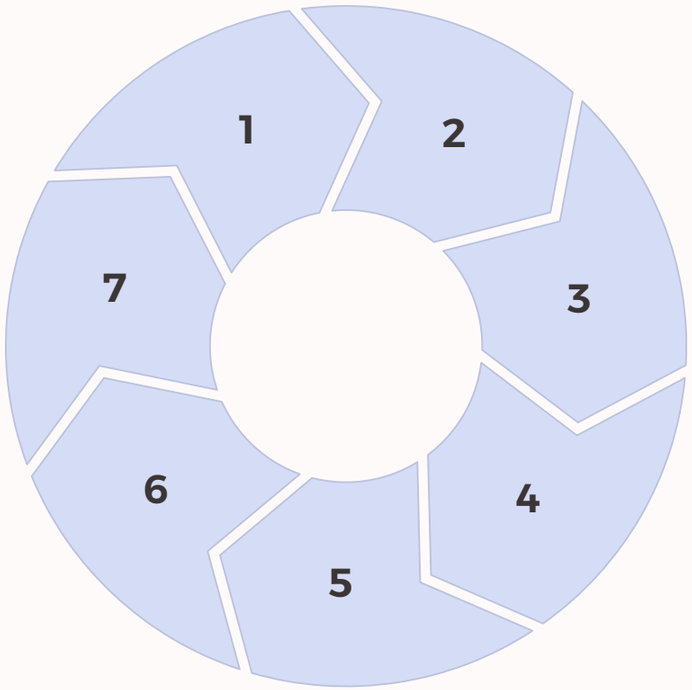
Cartographie des risques, scénarios de crise

7. Agir

Mise en œuvre des procédures, communication, retour à la normale

6. Alerter

Activation cellule de crise, notification autorités



2. Veille des Risques

Veille sécuritaire, géopolitique, cyber (CERT-FR)

3. Planifier

PGC, PCA, PRA, plans sectoriels

4. Former et S'entraîner

Exercices de simulation, formation des équipes

5. Incident

Détection, qualification, escalade

01

Analyser et prévenir

Cartographie des risques, scénarios de crise.

02

Assurer une veille des risques

Veille sécuritaire, géopolitique, cyber (CERT-FR, ANSSI).

03

Planifier

PGC, PCA, PRA, plans sectoriels.

04

Former et s'entraîner

Exercices de simulation, formation des équipes.

05

Incident — Détecter et qualifier

Détection, qualification, escalade.

06

Alerter

Activation de la cellule de crise, notification des autorités.

07

Agir

Mise en œuvre des procédures, communication, retour à la normale.

Bilan d'Après-Crise et Amélioration Continue

RETEX — Retour d'Expérience

Analyse systématique des causes, des délais de détection et de réponse, des lacunes organisationnelles révélées par la crise.

Indicateurs à mesurer

MTTD

Mean Time To Detect

MTTR

Mean Time To Respond/Recover

Coût

Coût total de l'incident

Réputation

Impact réputationnel mesuré

Mise à jour des plans

Révision du PGC, du PCA, des procédures — au minimum **annuellement** ou après chaque incident significatif.

Obligation NIS2

Rapport final d'incident à l'ANSSI dans le **mois** suivant l'incident.

Partage d'information

Participation aux ISAC (Information Sharing and Analysis Centers) sectoriels — recommandé par l'ANSSI pour renforcer la résilience collective.

PARTIE 4

Conformité Réglementaire 2027

DUERP, plans de prévention, passeport de prévention et consignes incendie — le socle documentaire obligatoire.

Le Document Unique d'Évaluation des Risques Professionnels (DUERP)

Document Unique

Inventaire des risques par unité de travail, obligatoire dès le 1er salarié

Inventaire des Risques

Identification exhaustive de tous les dangers par poste

Cotation

Évaluation probabilité × gravité pour prioriser les actions

Mesures de Prévention

Actions correctives et préventives planifiées

Programme Annuel

Planification et suivi des actions de prévention

Obligation légale

Art. R4121-1 du Code du travail — obligatoire pour toute entreprise dès le **1er salarié**. Sanction : amende jusqu'à **1 500 € par salarié** en cas d'absence ou d'insuffisance.

Évolution loi Santé au travail (2021)

- Conservation du DUERP pendant **40 ans**
- Dépôt sur portail numérique (déployé progressivement depuis 2022)

Contenu obligatoire

- Inventaire des risques par unité de travail
- Cotation probabilité × gravité
- Mesures de prévention associées
- Programme annuel de prévention

PST 2026-2030 — Nouvelles obligations

Renforcement de l'évaluation différenciée selon le sexe, prise en compte des risques émergents :

- Risques liés à l'IA au travail
- Risques du télétravail intensif
- Risques climatiques (chaleur extrême)
- Adaptation des EPI aux femmes
- Lutte contre les violences sexuelles et sexistes au travail (VSST)

Plan de Prévention et PPSPS

Document PPSPS

Plan Particulier de Sécurité et de Protection de la Santé

Casque de Sécurité

Équipements de Protection Individuelle (EPI) obligatoires

Zone de Travaux

Délimitation et signalisation du chantier

Plan de Prévention

Document signé entre entreprise utilisatrice et entreprise extérieure

Protocole de Sécurité

Pour les opérations de chargement/déchargement

Plan de prévention

Obligatoire pour les travaux réalisés par une entreprise extérieure (EE) dans les locaux d'une entreprise utilisatrice (EU) — Art. R4512-6 à R4512-12 Code du travail. Seuil : travaux dangereux ou opérations **>400 heures sur 12 mois**.

PPSPS

Plan Particulier de Sécurité et de Protection de la Santé — obligatoire sur les chantiers BTP, rédigé par chaque entreprise intervenante.

Protocole de sécurité

Document écrit pour les opérations de chargement/déchargement — signé par l'entreprise d'accueil et le transporteur.

Évolution 2027

Intégration des **risques cyber** dans les plans de prévention pour les prestataires ayant accès aux systèmes d'information de l'entreprise.

Consignes de Sécurité Incendie — Mise à Jour Réglementaire

Chiffres clés 2027

1/4

Non formés

Français non formés aux gestes de sécurité incendie

1/3

Ignorent

Ignorent les mesures anti-incendie sur leur lieu de travail

2,3 Md€

Dommages/an

Dommages incendie annuels en France — 1ère cause de sinistres majeurs

Obligations réglementaires

- Consignes incendie selon la norme **NF EN ISO 7010** — désormais applicables à **tous les établissements**
- Équipements d'extinction disponibles et identifiés
- Moyens d'alerte clairement indiqués
- Nom des personnes chargées d'alerter les pompiers

Formation obligatoire

- Exercice d'évacuation au moins **1 fois/an**
- Formation des équipiers de première intervention (EPI)

Base légale : Art. R232-12-1 à R232-12-29 du Code du travail.

Passeport de Prévention — Nouvelle Obligation 2026

1

Avril 2025

Ouverture aux organismes de formation.

2

Mars 2026

Ouverture aux employeurs — obligation de déclarer toutes les formations SST dispensées.

3

Novembre 2026

Ouverture aux travailleurs — accès à leur espace personnel.

4

2027

Pleine opérationnalité — décret n° 2026-496 du 12 juin 2026 : période transitoire adaptée.

Fonctionnement

Centralise toutes les formations en santé et sécurité au travail (SST) suivies par chaque travailleur, tout au long de sa carrière. Créé par la **loi du 2 août 2021** (réforme santé au travail).

Utilité pratique

- Traçabilité des compétences sécurité
- Valorisation lors des recrutements
- Preuve de conformité en cas de contrôle
- Outil central du PST 2026-2030

PARTIE 5 — NOUVELLE SECTION 2027

Nouvelles Réglementations 2023-2027

NIS2, AI Act, DORA, PST 2026-2030 — le paysage réglementaire radicalement transformé.

Directive NIS2 et Loi Résilience — Révolution Cyber

NIS2 en chiffres

~15K

Entités concernées

En France sur 18 secteurs (vs ~500 sous NIS1)

10 M€

Amende max EE

Ou 2% du CA mondial pour les Entités Essentielles

7 M€

Amende max EI

Ou 1,4% du CA pour les Entités Importantes

Calendrier et transposition

- Directive UE 2022/2555 — entrée en vigueur **octobre 2024**
- Transposition française via la **loi Résilience** — retard pris : renvoyée à l'automne 2026
- La Commission européenne a renvoyé la France devant la CJUE le **8 juillet 2026** pour défaut de transposition

2 catégories d'entités

- **Entités Essentielles (EE) :** ≥250 salariés ou CA ≥50 M€
- **Entités Importantes (EI) :** ≥50 salariés ou CA ≥10 M€

Loi Résilience — périmètre élargi

Transpose également DORA (secteur financier) et la directive REC (résilience des entités critiques).

Obligations NIS2 — Ce que Doit Faire Votre Entreprise

1 Auto-enregistrement

S'enregistrer auprès de l'ANSSI via le portail **MonEspaceNIS2**.

2 Mesures de sécurité (Art. 21 NIS2)

Politique de sécurité SI, gestion des incidents, continuité d'activité, sécurité de la chaîne d'approvisionnement, chiffrement, contrôle d'accès, **MFA**.

3 Notification d'incidents

Alerte précoce **24h**, notification complète **72h**, rapport final **1 mois** à l'ANSSI.

4 Responsabilité des dirigeants

Les organes de direction peuvent être tenus personnellement responsables et **interdits d'exercer** en cas de manquement grave.

Référentiel ReCyF

Publié par l'ANSSI le 17 mars 2026 — guide pratique de mise en conformité NIS2.

Chaîne d'approvisionnement

Obligation d'évaluer la sécurité des fournisseurs et sous-traitants critiques — même s'ils ne sont pas directement soumis à NIS2.

18 Secteurs Concernés par NIS2

Secteurs hautement critiques

1. Énergie
2. Transport
3. Secteur bancaire
4. Infrastructures des marchés financiers
5. Santé
6. Eau potable
7. Eaux usées
8. Infrastructures numériques
9. Gestion des services TIC
10. Espace
11. Administrations publiques

Autres secteurs critiques

1. Services postaux et de courrier
2. Gestion des déchets
3. Produits chimiques
4. Denrées alimentaires
5. Industries manufacturières
6. Fournisseurs numériques
7. Recherche

Sous-traitants

Même non directement soumis à NIS2, les sous-traitants d'entités NIS2 doivent répondre à des exigences de sécurité contractuelles.

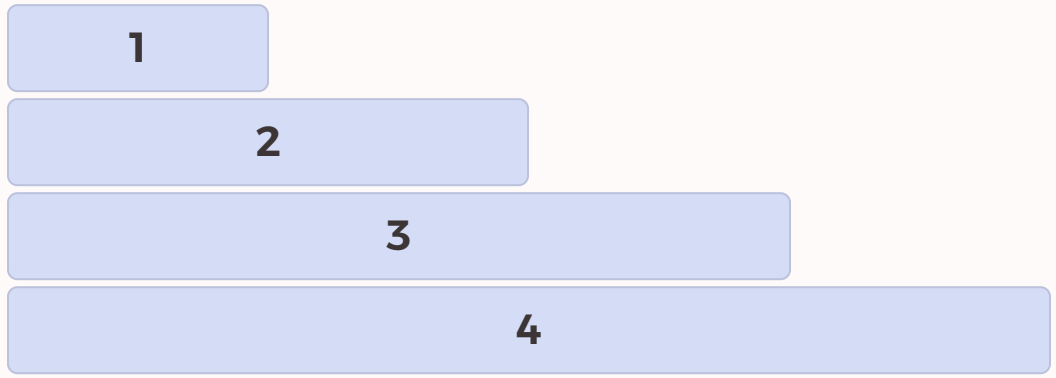
Vérifiez votre statut : test de maturité cyber ANSSI (3 min) sur **messervices.cyber.gouv.fr**

AI Act — Règlement Européen sur l'Intelligence Artificielle

Calendrier d'application

- Publié au JOUE le **12 juillet 2024**
- Application progressive depuis le **1er août 2024**
- Systèmes interdits : **février 2025**
- Règles complètes applicables : **août 2026**
- Omnibus IA (juillet 2026) : simplifications pour les PME

4 niveaux de risque



1 Risque minimal

Usage libre — filtres anti-spam, jeux vidéo IA.

2 Risque limité

Obligations de transparence — chatbots, deepfakes.

3 Haut risque

Recrutement, contrôle d'accès, sécurité des infrastructures critiques — obligations strictes.

4 Inacceptable

Interdit : notation sociale, manipulation subliminale, identification biométrique en temps réel (sauf exceptions).

⚠ **Impact sécurité :** les systèmes de vidéosurveillance intelligente, de contrôle d'accès biométrique et de détection comportementale sont classés à **haut risque** — obligations de documentation, audit et supervision humaine.

RGPD & IA — Nouvelles Obligations 2025-2027

Principe fondamental

L'IA ne bénéficie d'**aucune exemption au RGPD**. Dès qu'un système d'IA traite des données personnelles — à l'entraînement, en production ou en sortie — le règlement s'applique intégralement.

3 moments du cycle de vie IA concernés

1. Entraînement des modèles
2. Fonctionnement opérationnel
3. Données de sortie

Doctrine CNIL 2025

Recommandations sur l'analyse du statut RGPD des modèles IA, sécurité du développement, annotation des données d'entraînement — fiches IA publiées progressivement.

Obligations clés

Art. 6

Base légale du traitement

Art. 35

AIPD pour les traitements à haut risque

Art. 22

Encadrement des décisions automatisées

Vidéosurveillance IA

Double conformité **RGPD + AI Act** requise pour les systèmes d'analyse comportementale — AIPD obligatoire avant tout déploiement.

DORA — Résilience Opérationnelle Numérique du Secteur Financier

Gestion des risques TIC

Cadre complet de gestion des risques liés aux technologies de l'information et de la communication.

Gestion des incidents

Délais stricts de notification aux autorités (ACPR, AMF).

Tests de résilience

TLPT (Threat-Led Penetration Testing) obligatoires pour les entités financières significatives.

Gestion des risques tiers

Registre obligatoire de tous les prestataires TIC critiques — cartographie complète.

Partage d'informations

Participation aux mécanismes de partage d'informations sur les cybermenaces.

Règlement (UE) 2022/2554 — applicable depuis janvier 2025. Concerne : banques, assurances, sociétés de gestion, prestataires de paiement. Transposé en France via la loi Résilience (cohérence avec NIS2 et REC).

Plan Santé au Travail 2026-2030 — Nouvelles Priorités

Lancement — 5 juin 2026

Fusion avec le Plan de Prévention des Accidents du Travail Graves et Mortels (PATGM). Co-construit avec les partenaires sociaux et institutionnels.

Axe central

Décloisonnement des politiques de santé au travail — meilleure continuité entre médecine du travail, médecine de ville et hôpital.

3 priorités majeures

1 Accidents graves et mortels

Focus sur les jeunes travailleurs et les intérimaires — publics les plus exposés.

2 Santé des femmes au travail

Évaluation des risques différenciée selon le sexe, lutte contre les VSST, adaptation des EPI.

3 Risques émergents

IA au travail, télétravail intensif, risques climatiques (chaleur extrême), risques psychosociaux.

PARTIE 6

Risque Malveillance et Sûreté

Auteurs, typologies, ingénierie sociale et zonage — maîtriser la menace intentionnelle.

Éléments d'Attractivité et Ingénierie Sociale

Hameçonnage

Emails frauduleux ciblant les collaborateurs

Vishing

Appels téléphoniques frauduleux (voix clonée par IA)

Hypertrucage (Deepfake)

Vidéos falsifiées de dirigeants pour fraude

Prétexte

Scénario inventé pour obtenir des informations

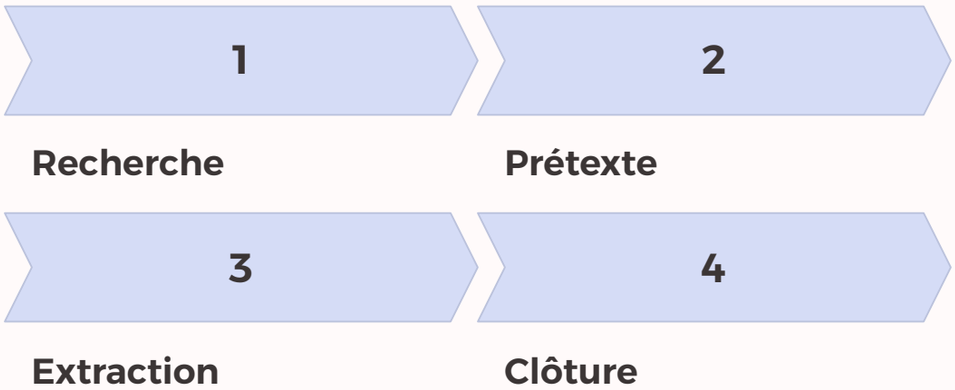
Extraction

Récupération des données ou virements frauduleux

Facteurs d'attractivité

- Pays représenté et image (cibles activistes)
- Emplois générés
- Savoir-faire et secrets industriels
- Valeurs présentes (numéraires, matières premières)
- Personnalités (COMEX, VIP)
- Sous-traitants — cibles privilégiées car plus vulnérables

Ingénierie sociale — 4 étapes



Nouvelles formes 2027

- **Vishing par IA :** voix clonée du DG pour autoriser un virement
- **Deepfake vidéo :** fraude au président par visioconférence falsifiée
- **Spear phishing LLM :** emails ultra-personnalisés générés par IA

Fraude au président

485 M€ de pertes en France en 2024 selon la Banque de France — manipulation psychologique assistée par IA générative.

Environnements et Contextes Extérieurs de l'Entreprise

Environnement Naturel et Urbain

Accessibilité (routes, voies ferrées), isolement, climatologie

Environnement Socio-Économique

Contexte social local, géopolitique, économique

Environnement Législatif

Code du travail, ICPE/SEVESO, NIS2, CNIL, Code de la Sécurité Intérieure

Environnement naturel/urbain

Accessibilité (routes, autoroutes, voies ferrées, cours d'eau), isolement (rural vs urbain), climatologie — brouillard et neige contraignent la détection périmétrique.

Environnement socio-économique

Contexte social local (délinquance), géopolitique (pays d'implantation, relations avec la France), conjoncture économique (risques de marché).

Cadre législatif applicable

- Code du travail (Art. L4121-1)
- Code de l'environnement (ICPE/SEVESO)
- Code de la construction (ERP, IGH)
- Réglementations SAIV, ESSP, Code de la Sécurité Intérieure
- CNIL, NIS2, AI Act

Risques climatiques 2027

Canicules (impact sur les équipements de détection), inondations (locaux techniques), tempêtes — intégration obligatoire dans le DUERP et le PCA.

Auteurs d'Actes de Malveillance

Acteurs Étatiques

Espionnage industriel commandité par des États (DGSI 2024-2026).

Cybercriminels

Groupes organisés (ransomware-as-a-service), hacktivistes.

Terroristes

Attaques physiques et cyber sur les infrastructures critiques.

Employés Malveillants

Sabotage interne, exfiltration de données, fraude.

Concurrents

Espionnage industriel, débauchage de talents, vol de PI.

Grand Banditisme

Vols organisés, cambriolages, extorsion.



Acteurs étatiques

Espionnage industriel commandité par des États — selon les rapports DGSI 2024-2026.



Cybercriminels

Groupes organisés (ransomware-as-a-service), hacktivistes, script kiddies.



Terroristes

Attaques physiques et cyber sur les infrastructures critiques.



Employés mécontents

Sabotage interne, exfiltration, fraude — risque amplifié par le télétravail.



Nouveauté 2027 — IA offensive

Acteurs utilisant l'IA générative pour automatiser et industrialiser les attaques à grande échelle.

Typologies des Actes de Malveillance

Fraude

Fraude au président, fraude documentaire, escroquerie.

Vol

Vol à main armée, cambriolage, vol interne, vol de données.

Terrorisme

Attentat, sabotage d'infrastructure, cyberterrorisme.

Activisme

Sabotage, intrusion, dégradation, désinformation.

Corruption

Corruption d'agents publics ou privés, trafic d'influence.

Atteintes au Personnel

Agression, séquestration, harcèlement.

Atteintes au Site

Intrusion, dégradation, incendie volontaire.

Cyber

Rançongiciel, hameçonnage, DDoS, espionnage, sabotage OT.

Analyse et Gestion des Flux

Zone Périphérique

Accès public, périmètre extérieur

Zone Périmétrique

Accès contrôlé, enveloppe du bâtiment

Zone Courante

Accès restreint aux salariés et visiteurs autorisés

Zone Critique

Accès très restreint, actifs sensibles

Flux à gérer

- Personnes : salariés, visiteurs, prestataires
- Véhicules : LAPI (Lecture Automatique de Plaques)
- Marchandises : protocoles de sécurité
- Données numériques : accès VPN, ZTNA

Outils de contrôle

Badgeage, sas de sécurité, LAPI, vidéosurveillance analytique.

Nouveauté 2027 — Convergence cyber-physique

Gestion des flux numériques (ZTNA — Zero Trust Network Access) intégrée à la politique de contrôle d'accès physique. Démarche partenariale avec les référents sûreté police/gendarmerie et le CDSE.

Concept de Protection des 3 Cubes et Zonage de Sûreté

3 zones concentriques



1 Zone Périphérique

Périmètre extérieur — première barrière.

2 Zone Périmétrique

Enveloppe du bâtiment — deuxième couche.

3 Zone de Valeur

Actifs à protéger — cœur sensible.

Zonage de sûreté — code couleur

- **Bleue :** Zone Publique
- **Jaune :** Zone Contrôlée
- **Orange :** Zone Restreinte
- **Rouge :** Zone Sensible

Application cyber

Le même principe s'applique aux réseaux informatiques : DMZ → réseau interne → réseau OT → zone ultra-sensible. Défense en profondeur : un intrus doit franchir plusieurs obstacles successifs.

Les 3 zones de protection

Zone Périphérique

Périmètre extérieur du site, clôtures, éclairage, détection périmétrique

Zone Périmétrique

Enveloppe du bâtiment, portes blindées, contrôle d'accès

Zone de Valeur

Actifs sensibles à protéger, coffres, serveurs, archives

Zonage de sûreté

Zone Publique

Accès libre, hall d'accueil, parking

Zone Contrôlée

Accès sur badge, bureaux, ateliers

Zone Restreinte

Accès nominatif, salles serveurs, R&D

Zone Sensible

Accès très restreint, direction, coffres

PARTIE 7

Systèmes de Sûreté Physique

Prévention situationnelle, détection d'intrusion, contrôle d'accès, vidéosurveillance et maintenance.

Prévention Situationnelle

Surveillance Naturelle

Conception favorisant la visibilité, élimination des angles morts

Contrôle Naturel des Accès

Aménagement guidant les flux vers les points de contrôle

Renforcement Territorial

Délimitation claire des espaces publics et privés

Maintenance

Entretien régulier signalant une présence active et dissuasive

Éclairage Stratégique

Illumination des zones sensibles, détection nocturne

Définition

Ensemble de mesures visant à réduire les opportunités de passage à l'acte par la conception et l'aménagement de l'environnement physique.

Principes CPTED

- Surveillance naturelle
- Contrôle naturel des accès
- Renforcement territorial
- Maintenance des espaces

ESSP — Obligation légale

Art. L114-1 Code de la sécurité intérieure — obligatoire pour les projets >5 000 m² ou >100 logements.

Aménagements recommandés

- Éclairage adapté et sans zones d'ombre
- Végétation maîtrisée (pas de cachettes)
- Signalétique claire et dissuasive
- Mobilier urbain anti-intrusion (bornes, blocs béton)

Référent Sûreté

Interlocuteur police/gendarmerie spécialisé PTM — ressource gratuite pour les entreprises.

Détection d'Intrusion et Protection Mécanique

Détecteur d'Intrusion

Capteurs infrarouges passifs (PIR), micro-ondes, double technologie

Panneau d'Alarme

Centrale de détection avec transmission aux forces de l'ordre

Serrure Électronique

Contrôle d'accès électronique certifié A2P

Capteur de Mouvement

Détection périmétrique et volumétrique

Couches de Sécurité

Principe de défense en profondeur, délai de résistance mécanique

3 niveaux de détection

01

Périphérie

Approche et pénétration — barrières IR, câbles vibratoires, radars, analyse vidéo.

02

Périmétrie

Mouvements internes — détecteurs PIR, micro-ondes, double technologie.

03

Zone des valeurs

Protection ultime — détection de proximité, coffres, alarmes volumétriques.

Protection mécanique

- Portes blindées, vitrages feuilletés
- Coffres-forts, serrures certifiées A2P
- Grilles, barreaux, volets roulants sécurisés

Principe fondamental : le délai de résistance mécanique doit être supérieur au délai d'intervention des forces de l'ordre. Normes : NF EN 50131 (alarmes), NF EN 1627 (résistance à l'effraction).

Contrôle d'Accès — Technologies et Réglementation

Lecteur Biométrique

Empreinte digitale, reconnaissance faciale, iris

Badge RFID

Carte sans contact, technologie NFC

Clavier Code

Code PIN, authentification à facteurs multiples

Serrure Électronique

Contrôle centralisé des accès

Journal d'Accès

Traçabilité complète des entrées/sorties

Technologies disponibles

- Badge/carte RFID, code PIN
- Biométrie : empreinte, visage, iris
- Tourniquet, sas de sécurité, LAPI

Biométrie — encadrement strict

- **RGPD Art. 9 :** données sensibles — AIPD obligatoire
- **AI Act :** identification biométrique à distance en temps réel en espace public = interdit

Contrôle d'accès logique 2027

- **MFA** obligatoire pour tous les accès SI sensibles (NIS2)
- **Zero Trust :** "ne jamais faire confiance, toujours vérifier" — recommandé ANSSI
- **PAM :** gestion des comptes à privilèges
- Revue trimestrielle des droits d'accès — principe du moindre privilège

RGPD-CNIL et Systèmes de Sûreté — Mise à Jour 2027

Vidéosurveillance

Information des personnes filmées obligatoire (panneaux), durée de conservation limitée (max **30 jours** en général), accès restreint aux enregistrements.

Autorisation préfectorale

Obligatoire pour la vidéoprotection sur la voie publique ou dans les lieux ouverts au public (Art. L251-1 Code de la sécurité intérieure).

Biométrie

AIPD (Analyse d'Impact sur la Protection des Données) obligatoire avant tout déploiement — consentement ou nécessité absolue de sécurité à démontrer à la CNIL.

Drones

Réglementation DGAC (arrêté du 3 décembre 2020 modifié) + RGPD si captation d'images de personnes identifiables.

IA analytique

Double conformité **RGPD + AI Act** pour les systèmes d'analyse comportementale ou de reconnaissance faciale — haut risque AI Act.

Vidéosurveillance et Vidéoprotection

Caméra IP

Haute définition 4K, vision nocturne, résistance aux intempéries

Enregistreur NVR

Stockage sécurisé des enregistrements vidéo

Écran de Surveillance

Monitoring en temps réel par les agents

Stockage 30 Jours

Durée maximale légale de conservation (CNIL)

Analyse IA

Détection automatique d'intrusion, comportements suspects

Distinction fondamentale

Vidéosurveillance : usage privé, intérieur — autorisation interne suffit.

Vidéoprotection : espace public — soumise à autorisation préfectorale.

Évolution technologique

- Caméras 4K — haute résolution pour l'identification
- Analyse vidéo par IA : détection d'intrusion, comptage, comportement anormal
- Caméras thermiques — détection nocturne sans éclairage

Caméras à analyse IA – Réglementation

Classées à **haut risque** sous l'AI Act si elles analysent des comportements ou identifient des personnes — obligations de documentation, enregistrement et supervision humaine.

Drones de surveillance

Usage professionnel encadré par la DGAC — catégories A1/A2/A3 selon masse et zone de vol. Double conformité DGAC + RGPD.

Conservation

30 jours maximum pour les enregistrements (sauf réquisition judiciaire ou flagrant délit).

Approche Méthodologique des Systèmes de Sûreté

Phase 1 — Analyse de Risque

Identification des valeurs à protéger, des menaces, des vulnérabilités, définition du niveau de sécurité cible.

Phase 2 — Conception

Choix des technologies, architecture du système, intégration contrôle d'accès / alarme / vidéo.

Phase 3 — Réalisation

Installation par des professionnels certifiés (APSAD, CNPP), recette du système, formation des utilisateurs.

Phase 4 — Maintenance

Maintenance préventive planifiée, mise à jour des firmwares, tests réguliers — registre de sûreté tenu à jour.

⚠ **Intégration cyber-physique :** les systèmes de sûreté physique (caméras IP, contrôle d'accès connecté) sont des vecteurs d'attaque cyber — leur sécurisation est obligatoire sous NIS2.

Maintenance des Installations de Sûreté

Référentiels APSAD

- **R6** — Alarmes anti-intrusion
- **R7** — Vidéosurveillance
- **R8** — Contrôle d'accès
- **R81** — Drones de surveillance

Traçabilité obligatoire

Chaque équipement marqué d'un code-barres d'identification — rapports de visites consultables dans le registre de sûreté.

Maintenance préventive

Vérification et entretien complet des installations selon un planning défini — réduit la probabilité de défaillance et maintient la conformité réglementaire.

Maintenance corrective

Délais d'intervention contractuels à maîtriser pour ne pas vulnérabiliser l'entreprise pendant la période de réparation.

Cybersécurité des équipements

Mise à jour régulière des **firmwares** des caméras IP, contrôleurs d'accès et centrales d'alarme — vecteurs d'attaque fréquents exploités par les cybercriminels.

Registre de sûreté

Document obligatoire retraçant toutes les interventions, vérifications et incidents.

PARTIE 8

Cybersécurité

Panorama des cybermenaces, protection des systèmes d'information, résilience et conformité ANSSI.

Panorama de la Cybermenace 2027

Rançongiciel

Chiffrement des données avec demande de rançon, +50% en 2024

Hameçonnage

Emails frauduleux, spear phishing ultra-ciblé par IA

Chaîne d'Approvisionnement

Attaques via les fournisseurs et sous-traitants

Systèmes OT et IoT

Ciblage des systèmes industriels SCADA et automates

IA Offensive

Automatisation des attaques, exploitation de vulnérabilités zero-day

Menaces dominantes

- Ransomware (rançongiciels) — paralysie totale des activités
- Phishing / spear phishing — 1er vecteur d'intrusion
- Compromission de comptes (credential stuffing)
- Attaques supply chain — 3 parties prenantes touchées simultanément

Données clés ANSSI 2025-2026

- **1 366 incidents** portés à la connaissance de l'ANSSI en 2025
- **+50%** des cyberattaques exploitent des vulnérabilités d'équipements "en bordure" (pare-feux, VPN)
- Maturité cyber des organisations françaises encore insuffisante (baromètre ANSSI mars 2026)

Nouvelles menaces IA offensive

Phishing généré par LLM, deepfakes audio/vidéo, automatisation des attaques, exploitation de vulnérabilités zero-day par IA.

Attaques OT/IoT

Ciblage des systèmes industriels (SCADA, automates) — impact physique potentiel sur la production.

Risques Liés à la Mobilité et au Télétravail

Équipements nomades

PC portables, smartphones, tablettes — vecteurs d'attaque privilégiés. Mesures : chiffrement disque dur (BitLocker, FileVault), câble antivol, filtre de confidentialité d'écran, verrouillage automatique.

Télétravail — surface élargie

Explosion post-COVID. Réseaux domestiques non sécurisés, shadow IT, accès depuis des équipements personnels non maîtrisés.

VPN et ZTNA

VPN obligatoire pour les accès distants. Migration vers le **Zero Trust Network Access** recommandée par l'ANSSI pour les entités NIS2.

MDM

Mobile Device Management — gestion centralisée des équipements mobiles, effacement à distance en cas de perte ou vol.

Règles d'hygiène en déplacement

- Ne pas utiliser les bornes USB publiques (juice jacking)
- Éviter les réseaux Wi-Fi publics — utiliser un hotspot personnel
- Utiliser un téléphone dédié dans les pays à fort risque d'espionnage

Sensibilisation et Formation des Collaborateurs

Le facteur humain — chiffre clé

90%

Erreur humaine

Des incidents cyber impliquent une erreur humaine (phishing, mot de passe faible, mauvaise configuration)

L'humain est **à la fois le maillon faible et le premier rempart** de la cybersécurité.

Programme de sensibilisation

- Formation initiale à l'embauche
- Formations régulières (au moins annuelles)
- Simulations de phishing contrôlées
- Affichage de bonnes pratiques
- Intégration dans le **Passeport de prévention**

Réflexes à inculquer

- Signaler tout incident suspect immédiatement
- Ne pas cliquer sur les liens douteux
- Vérifier l'identité des demandeurs (appel de confirmation)
- Ne jamais brancher une clé USB inconnue

Objectif 2027

Faire de la cybersécurité un réflexe au même titre que la sécurité incendie — **culture cyber ancrée** dans toute l'organisation.

Authentification et Ressources du Système d'Information



MFA — Obligatoire

Authentification multi-facteurs pour tous les accès aux applications critiques, VPN, messagerie. Obligation NIS2 et recommandation ANSSI.



Gestion des mots de passe

Gestionnaire d'entreprise (Dashlane Business, Keeper), politique de complexité, renouvellement sur compromission avérée.



Comptes à privilèges (PAM)

Comptes administrateurs isolés, sessions enregistrées, principe du moindre privilège — revue trimestrielle.



Segmentation réseau

Isolation des réseaux OT/IT, VLAN, DMZ — limiter la propagation latérale en cas d'intrusion.



Sauvegarde 3-2-1

3 copies, 2 supports différents, 1 hors site — testée régulièrement. Règle d'or anti-ransomware.

L'ANSSI et le Plan Stratégique 2025-2027

5 missions de l'ANSSI

- **Défendre**
- **Connaître**
- **Partager**
- **Accompagner**
- **Réguler**

Référentiel ReCyF — Mars 2026

Guide pratique de mise en conformité NIS2 — publié le 17 mars 2026 par l'ANSSI.

Ressources disponibles gratuitement

- **cyber.gouv.fr** — guides et référentiels
- **MonEspaceNIS2** — enregistrement et conformité
- **CERT-FR** — alertes et avis de sécurité (abonnement recommandé)
- **SecNumCloud** — qualification cloud souverain

Accompagnement PME

- Dispositif Cyber PME — diagnostic gratuit
- Prestataires qualifiés PRIS (Réponse aux Incidents)
- Test de maturité cyber (3 min) sur messervices.cyber.gouv.fr

ISO 27001 — Certification Sécurité de l'Information

Norme ISO/IEC 27001:2022

Système de Management de la Sécurité de l'Information (SMSI) — applicable à toute organisation. Couvre la **confidentialité, intégrité et disponibilité** des informations.

Processus de certification

Mise en œuvre
Appliquer les 93 contrôles requis par la norme.

Audit interne
Vérifier conformité et efficacité du SMSI.



Analyse des risques
Identifier et évaluer les risques informationnels.

Audit de certification
Évaluation par un organisme accrédité.

93 contrôles — 4 thèmes (version 2022)

Organisationnel

Politiques, rôles, responsabilités

Humain

Formation, sensibilisation, gestion des accès

Physique

Sécurité des locaux et équipements

Technologique

Chiffrement, journalisation, tests

Lien NIS2 et Cyber Resilience Act

La certification ISO 27001 facilite la conformité NIS2. Le **Cyber Resilience Act (CRA)** — règlement européen sur la cybersécurité des produits connectés — est pleinement applicable en 2027.

PARTIE 9

Conformité Documentaire et Organisationnelle

Règlement intérieur, chartes, clauses contractuelles et protection de la propriété industrielle.

Le Règlement Intérieur

Obligation légale

Art. L1311-2 Code du travail — obligatoire pour les entreprises de **50 salariés et plus**.

Procédure

1. Consultation du CSE
2. Dépôt à l'inspection du travail
3. Affichage dans les locaux

Risque de non-conformité

Règlement intérieur non conforme = sanctions disciplinaires **inopposables** aux salariés.

Contenu obligatoire

- Règles d'hygiène et de sécurité
- Discipline et sanctions
- Harcèlement moral et sexuel
- Droits de la défense

Évolutions 2027 — Nouvelles clauses recommandées

- Règles d'utilisation de l'IA générative au travail (ChatGPT, Copilot)
- Politique de télétravail
- Règles de cybersécurité (charte informatique annexée)
- Clause de confidentialité intégrée ou annexée

Livret d'Accueil Sécurité et Registre Santé-Sécurité

Livret d'accueil sécurité

Remis à tout nouveau salarié et prestataire — consignes d'évacuation, numéros d'urgence, règles de sécurité spécifiques au site. Premier document de conformité.

Registre santé-sécurité

Permet à tout salarié de consigner ses observations sur la sécurité — consulté par le CSE et l'inspection du travail. Outil de dialogue social.

Registre de sûreté

Trace toutes les interventions sur les systèmes de sûreté, les incidents, les vérifications périodiques — obligatoire pour les systèmes APSAD.

Registre de sécurité incendie

Obligatoire — consigne les vérifications des installations, les exercices d'évacuation, les formations EPI. Présenté lors des visites de la commission de sécurité.

Nouveauté 2027 : numérisation des registres recommandée — accessibilité, traçabilité, archivage sécurisé. Durée de conservation du DUERP : **40 ans**.

Clauses de Non-Concurrence et de Confidentialité

Clause de non-concurrence — 5 conditions cumulatives

1. Indispensable à la protection des intérêts de l'entreprise
2. Contrepartie financière obligatoire
3. Limitée dans l'espace
4. Limitée dans le temps
5. Prise en compte des spécificités de l'emploi

Clause de confidentialité

Protège les informations sensibles (savoir-faire, données clients, stratégie) — sans limitation de durée possible. Mesures techniques associées : DLP (Data Loss Prevention).

Loi sur le secret des affaires (2018)

Transposition de la directive UE 2016/943 — protection renforcée du savoir-faire et des informations commerciales confidentielles non brevetées.

Nouveauté 2027 — IA et propriété intellectuelle

Protection des **données d'entraînement IA** et des modèles propriétaires — nouveau champ d'application du secret des affaires. Question ouverte : qui est titulaire des droits sur les créations générées par IA ? Évolution jurisprudentielle en cours.

Charte Informatique et Protection des Données

Statut juridique

Définit les règles d'utilisation des ressources informatiques — **obligatoirement annexée au règlement intérieur** pour être opposable aux salariés.

Contenu 2027 — Nouvelles thématiques

- Utilisation des équipements professionnels et personnels
- Accès internet, messagerie, réseaux sociaux
- **IA générative (ChatGPT, Copilot) :** données confidentielles à ne pas saisir, vérification des outputs, responsabilité de l'utilisateur
- BYOD (Bring Your Own Device)
- Télétravail — règles spécifiques

DLP — Data Loss Prevention

Outils techniques pour prévenir la fuite de données :

- Surveillance des transferts de fichiers
- Blocage des clés USB non autorisées
- Contrôle des envois emails vers l'extérieur
- Journalisation des accès aux données sensibles

BYOD — Politique recommandée

MDM obligatoire, **cloisonnement** des données professionnelles et personnelles, droit d'effacement à distance des données d'entreprise.

Protection de la Propriété Industrielle

Brevets

Protection des inventions — dépôt INPI (France), OEB (Europe), PCT (international). Durée : **20 ans**.

Marques

Protection des signes distinctifs — dépôt INPI, EUIPO (UE). Renouvelable **indéfiniment**.

Dessins et modèles

Protection de l'apparence des produits — dépôt INPI. Durée : 5 ans renouvelable jusqu'à 25 ans.

Droits d'auteur

Protection automatique des œuvres originales (logiciels, bases de données, créations). Durée : **70 ans** après décès de l'auteur.

Secret des affaires

Loi du 30 juillet 2018 — protection du savoir-faire non breveté et des informations commerciales confidentielles.

IA — Question ouverte 2027

Titularité des droits sur les créations générées par IA — évolution jurisprudentielle en cours en France et en Europe.

Procédures SOP et Plans Opérationnels

SOP

Standard Operating Procedure — procédures opérationnelles normalisées étape par étape.

POI

Plan d'Opération Interne — gestion des accidents industriels, obligatoire pour les sites ICPE.

Plan de Sûreté

Document stratégique décrivant l'organisation et les mesures de sûreté du site.

PPI

Plan Particulier d'Intervention — plan préfectoral pour les accidents majeurs des sites SEVESO seuil haut.

PPMS

Plan Particulier de Mise en Sûreté — confinement pour les établissements scolaires et ERP.

PSO

Plan de Sûreté Opérationnel — déploiements à l'international en zones à risque.

PARTIE 10

Sûreté à l'International

Protection des ressortissants à l'étranger, analyse risque pays et gestion de crise internationale.

Sûreté des Ressortissants à l'Étranger

Analyse Pays

Évaluation géopolitique, sécuritaire, sanitaire, juridique avant départ

Briefing Sécurité

Formation aux risques spécifiques du pays de destination

Inscription Ariane

Enregistrement auprès de l'ambassade française (France Diplomatie)

VPN Sécurisé

Chiffrement des communications, protection des données

Téléphone Dédié

Appareil vierge sans données sensibles pour les pays à risque

Rapatriement

Procédures d'évacuation et contacts d'urgence locaux

Obligation de l'employeur

Devoir de protection des salariés en déplacement à l'étranger — Art. L4121-1 Code du travail. Responsabilité engagée en cas de manquement.

Analyse risque pays — Sources

- **France Diplomatie (MEAE) :** Conseils aux voyageurs
- **OSAC (US) :** Overseas Security Advisory Council
- **Control Risks, Drum Cussac :** prestataires spécialisés

Contexte 2027

Multiplication des zones de conflit, risques d'enlèvement en hausse dans certaines régions — renforcement impératif des protocoles de sécurité.

Mesures préventives — avant le départ

- Briefing sécurité personnalisé (risques pays)
- Assurance rapatriement et assistance médicale
- Enregistrement auprès de l'ambassade (**Ariane** — système MEAE)
- Téléphone sécurisé et chiffré
- VPN activé en permanence

Gestion de crise internationale

- PSO — Plan de Sûreté Opérationnel
- Procédures d'évacuation prédéfinies
- Contacts d'urgence locaux identifiés

Bonnes Pratiques de Gestion des Risques à l'International

Avant le déploiement

Analyse risque pays, briefing sécurité, équipements adaptés, assurances, enregistrement Ariane.

Deux premières semaines

Contact avec les autorités locales, identification des ressources d'urgence, évaluation sur place.

Cybersécurité terrain

Ne pas utiliser les ordinateurs des hôtels, éviter les bornes USB publiques, utiliser un téléphone dédié dans les pays à risque.

Espionnage industriel

Appareils vierges sans données sensibles, VPN systématique, vigilance accrue dans les pays à fort risque.

Retour — RETEX

Retour d'expérience après chaque mission, mise à jour des procédures, formation continue des équipes.

PARTIE 11

Sécurité Incendie et Produits Dangereux

Réglementation ERT/ERP/IGH, entreposage et gestion des substances dangereuses.

Réglementation Sécurité Incendie 2027

Sprinklers

Extinction automatique par eau, obligatoire selon la surface et l'activité

Extincteur

Extinction manuelle, vérification annuelle obligatoire (APSAD R1)

Détecteur de Fumée

Détection précoce, déclenchement de l'alarme

Alarme Incendie

Système d'alerte des occupants et des secours

Sortie de Secours

Dégagement obligatoire, signalisation normalisée NF EN ISO 7010

3 régimes réglementaires

ERT

Établissements Recevant des Travailleurs — Code du travail

ERP

Établissements Recevant du Public — Code de la construction

IGH

Immeubles de Grande Hauteur — réglementation spécifique

Causes d'incendie

Négligence, imprudence, électricité, chauffage, échauffement, étincelles, fuites de produits chimiques, malveillance, causes naturelles.

Référentiels APSAD

- **R1** — Extincteurs portatifs
- **R4** — Robinets d'incendie armés (RIA)
- **R6** — Systèmes d'alarme
- **R13** — Sprinklers

Coût des dommages incendie : **2,3 Md€/an** en France — 1ère cause de sinistres majeurs en entreprise.

Entreposage de Produits Dangereux

Armoire Coupe-Feu

Stockage des liquides inflammables, norme EN 14470-1

Pictogrammes SGH

Signalisation des dangers chimiques selon le règlement CLP

Fiche de Données de Sécurité (FDS)

16 rubriques obligatoires, règlement REACH

Zone de Stockage

Séparation des produits incompatibles, ventilation adaptée

Ventilation

Extraction des vapeurs dangereuses, prévention des atmosphères explosives

Classification SGH/CLP — Pictogrammes obligatoires

- Explosifs
- Inflammables
- Comburants
- Toxiques
- Corrosifs
- Irritants
- Dangereux pour l'environnement

Fiche de Données de Sécurité (FDS)

Obligatoire pour tout produit chimique dangereux — **16 rubriques** réglementaires (règlement REACH).

Armoires coupe-feu

Stockage des liquides inflammables — normes **EN 14470-1**. Conditions strictes d'installation et de maintenance.

ICPE

Installations Classées pour la Protection de l'Environnement — déclaration, enregistrement ou autorisation préfectorale selon les seuils.

Sites SEVESO

- **Seuil bas :** politique de prévention des accidents majeurs
- **Seuil haut :** SGS, POI, PPI — réglementation renforcée

Mesures organisationnelles

Formation du personnel, procédures de stockage, plan d'urgence interne, exercices réguliers.

PARTIE 12

Acteurs et Ressources

Institutions étatiques, partenaires locaux et experts — l'écosystème de la sécurité-sûreté en France.

Les Acteurs Étatiques de la Sécurité-Sûreté

ANSSI

Cybersécurité nationale, NIS2, certification, CERT-FR.

DGSI

Contre-espionnage, contre-terrorisme, protection du patrimoine économique.

SGDSN

Coordination interministérielle, OIV, SAIV.

CNIL

RGPD, AI Act, vidéosurveillance, biométrie.

INPI

Brevets, marques, dessins et modèles.

DREAL/DRIRE

ICPE, sites SEVESO, autorisation d'exploiter.

Inspection du Travail

Contrôle DUERP, règlement intérieur, conditions de travail.

Les Acteurs Locaux et Partenaires

Référent Sûreté

Policier ou gendarme spécialisé PTM — diagnostic gratuit, conseils, ESSP. Service gratuit pour les entreprises.

CDSE

Club des Directeurs de Sécurité des Entreprises — réseau professionnel, bonnes pratiques, veille sécuritaire.

ADESS

Association des Experts en Sécurité et Sûreté — auteur du présent guide, expertise, formation, conseil.

CNPP

Centre National de Prévention et de Protection — certification APSAD, formation, audit sécurité incendie et sûreté.

Assureurs

Partenaires clés — exigences de sécurité, audit des risques, financement des investissements de protection.

CSE

Comité Social et Économique — consulté sur toutes les questions de santé, sécurité et conditions de travail.

L'Étude de Sûreté et de Sécurité Publique (ESSP)

Définition et obligation légale

Diagnostic de sûreté réalisé par un référent sûreté ou un expert agréé — évalue les risques et propose des mesures de prévention situationnelle.

Art. L114-1 Code de la sécurité intérieure — obligatoire pour les projets d'aménagement :

- Surface > **5 000 m²**
- Plus de **100 logements**

Contenu d'une ESSP

1. Analyse de l'environnement (urbain, socio-économique, risques)
2. Identification des risques spécifiques au projet
3. Recommandations architecturales (CPTED)
4. Recommandations organisationnelles
5. Plan d'action priorisé

Bénéfices

- Réduction des risques dès la conception
- Économies sur les mesures correctives
- Meilleure assurabilité du site

Évolution 2027

Intégration des **risques cyber** dans les ESSP — convergence croissante sécurité physique et cybersécurité.

Le Référent Sûreté

Statut et missions

Policier ou gendarme spécialisé en **Prévention Technique de la Malveillance (PTM)** — interlocuteur gratuit et de confiance pour les entreprises.

Comment le contacter

- Police nationale : via la DDSP (Direction Départementale de la Sécurité Publique)
- Gendarmerie nationale : via le groupement départemental

Complémentarité

Le référent sûreté travaille en lien avec les experts privés (ADESS, CNPP) et les assureurs pour une approche globale.

Nouveauté 2027

Développement des **référents sûreté cyber** dans certaines unités — convergence des expertises physique et numérique au sein des forces de l'ordre.

Sensibilisation des équipes

Le référent sûreté intervient directement auprès des équipes pour renforcer la culture sécurité en entreprise.

Accompagnement pour l'ESSP

Aide à la réalisation de l'Étude de Sûreté et de Sécurité Publique, en lien avec les exigences réglementaires.

Prestations gratuites

Diagnostic de Sûreté

Analyse gratuite du site, identification des vulnérabilités et recommandations.

Conseils en Aménagement

Préconisations CPTED, prévention situationnelle, aménagement sécurisé.

Sensibilisation

Formation des équipes aux risques de malveillance et aux bonnes pratiques.

Accompagnement ESSP

Aide à la réalisation de l'Étude de Sûreté et de Sécurité Publique.

Lien avec les Forces de l'Ordre

Interface directe avec la police nationale ou la gendarmerie.

PARTIE 13

Mise en Œuvre et Plan d'Action

Organisation humaine et technique, checklist de conformité 2027 et tableau de maturité.

Surveillance des Risques — Organisation Humaine et Technique

Directeur Sécurité-Sûreté (DSS)

Pilotage de la politique globale de sécurité

Agents de Sécurité

Surveillance physique, rondes, contrôle d'accès

SOC Cyber 24/7

Centre opérationnel de surveillance des menaces numériques

Référent Sûreté Interne

Correspondant sécurité par site

KPI et Indicateurs

Taux d'incidents, MTTD, MTTR, taux de conformité

Organisation humaine

- Directeur Sécurité-Sûreté (DSS/RSSI)
- Agents de sécurité et d'accueil
- Référent sûreté interne
- Correspondants sécurité par site
- Acteurs majeurs : Moyens Généraux, RH, HSE, Immobilier, Juridique

Composantes techniques

- Centrale de surveillance (télésurveillance)
- Vidéosurveillance analytique
- Contrôle d'accès centralisé
- Détection intrusion
- **SOC (Security Operations Center)** cyber — 24/7, externalisable

Suivi et amélioration

KPI mensuels, revue mensuelle, audit annuel, exercices de simulation — amélioration continue.

Checklist de Conformité 2027 — Priorités d'Action

✅ Conformité Sociale

- DUERP à jour (risques émergents inclus : IA, télétravail, climatiques)
- Passeport de prévention alimenté (toutes formations SST déclarées)
- Consignes incendie universelles (tous établissements)
- Registres (sûreté, sécurité incendie, santé-sécurité) à jour

✅ Conformité Cyber (NIS2)

- Vérifier si entité NIS2 sur messervices.cyber.gouv.fr
- S'enregistrer auprès de l'ANSSI (MonEspaceNIS2)
- Mettre en œuvre les mesures Art. 21 (MFA, chiffrement, PCA, supply chain)
- Plan de notification d'incidents (24h/72h/1 mois)

✅ Conformité Données

- Registre des traitements RGPD à jour
- AIPD pour les traitements à haut risque
- Conformité AI Act pour les systèmes IA utilisés

✅ Conformité Sûreté Physique

- ESSP réalisée ou planifiée
- Systèmes de sûreté maintenus (APSAD)
- Plan de sûreté documenté
- Exercices de crise réalisés (au moins 1/an)

✅ Conformité Propriété Intellectuelle

- Brevets déposés et maintenus
- Clauses de confidentialité en place
- Secret des affaires protégé (technique + contractuel)

Tableau de Bord de la Maturité Sécurité-Sûreté

1

Niveau 1 — Initial

Pas de politique formalisée. Réaction aux incidents uniquement. Conformité minimale.

2

Niveau 2 — Défini

Politique documentée. DUERP à jour. Formations de base. Systèmes de sûreté installés.

3

Niveau 3 — Géré

Processus de gestion des risques opérationnel. PCA/PGC testés. Conformité NIS2/RGPD en cours. **Objectif minimum pour les entités NIS2.**

4

Niveau 4 — Optimisé

Amélioration continue. SOC opérationnel. Certifications (ISO 27001, APSAD). Exercices réguliers. Culture sécurité ancrée. **Cible pour les Entités Essentielles.**

Auto-évaluation

Test de maturité cyber ANSSI (3 min) + diagnostic référent sûreté + audit DUERP.

Objectif 2027

Toutes les entités NIS2 doivent atteindre le **niveau 3 minimum** — les entités essentielles visent le **niveau 4**.

Votre Plan d'Action Sécurité-Sûreté 2027

1 Court terme — 0-3 mois

Vérifier l'assujettissement NIS2. Mettre à jour le DUERP (risques émergents). Alimenter le passeport de prévention. Auditer les systèmes de sûreté physique.

2 Moyen terme — 3-12 mois

Mise en conformité NIS2 (mesures Art. 21). Déployer le MFA. Réaliser une ESSP. Former les collaborateurs à la cybersécurité. Tester le PCA/PRA.

3 Long terme — 1-3 ans

Viser la certification ISO 27001. Déployer un SOC (interne ou externalisé). Intégrer la convergence cyber-physique. Développer une culture sécurité durable.

L'argument économique

Coût moyen d'un incident cyber : **97 000 €** pour une PME (CESIN 2024). Coût d'un incendie majeur : plusieurs millions d'euros. Le coût de la prévention est systématiquement inférieur au coût du sinistre.

Partenaires clés

- ANSSI — cyber.gouv.fr
- Référent sûreté (police/gendarmerie)
- ADESS — expertise sécurité-sûreté
- CNPP — certification APSAD
- Assureurs — financement et audit
- Prestataires qualifiés PRIS (réponse aux incidents)

Principe fondamental : la sécurité globale n'est pas une option — c'est une obligation légale, éthique et stratégique pour toute organisation en 2027.

Sources

GUIDE SÉCURISER SON ENTREPRISE — ADESS (Juin 2022, document source)

Décret du 12 juin 2026 : allongement de la période transitoire — Passeport de prévention

NIS2 en France 2026 : ce que change la loi Résilience

Directive NIS 2 - MesServicesCyber — ANSSI

IA et RGPD : guide de conformité 2026 + checklist

Découvrez la directive NIS 2 et passez à l'action ! — ANSSI

Le Plan Santé au travail 2026-2030 — Ministère du Travail et des Solidarités

NIS2 : votre PME est-elle concernée ? 18 secteurs, calendrier 2026, sanctions — AdevWeb

Entrée en vigueur du règlement européen sur l'IA : questions-réponses — CNIL

IA : la CNIL finalise ses recommandations sur le développement des systèmes d'IA — CNIL