sosafe

Checkliste à l'intention des décideurs informatiques pour l'implémentation de la DLP

Le guide complet pour implémenter la Data leak prevention

Résumé analytique

Cette checkliste va vous guider pas à pas dans l'implémentation d'une stratégie de Data leak prevention efficace. Elle contient :

- La description détaillée des différentes étapes d'implémentation avec les responsabilités correspondantes
- Des modèles de politiques de DLP et de plans de réponse en cas d'incident
- Des KPI mesurables pour suivre l'efficacité de la stratégie
- Un mappage de conformité avec le RGPD, la directive NIS2 et la norme ISO 27001
- Des critères pour évaluer les différents outils
- Des procédures d'analyse et d'audit

Délai à prévoir : 3 à 6 mois pour l'implémentation intégrale (selon la taille de l'entreprise)

1 Phase 1 : Préparation et inventaire (semaines 1 à 4)

1.1 Gestion des intervenants

- [ ] Monter une équipe de projet
  - Responsable : RSSI / direction informatique
  - Doit comprendre : sécurité informatique, service juridique/conformité, RH, organe de représentation des collaborateurs, délégué à la protection des données
  - Livrable : charte de projet incluant le budget, le calendrier et les responsabilités
- [ ] Obtenir l'adhésion de la direction
  - Évaluer le risque actuel (les dommages que pourrait faire une violation de données)
  - Analyse de rentabilité : retour sur investissement avec les amendes et les atteintes à la réputation qui auront été évitées
  - Ressources nécessaires : budget, ETP, consultant externe
- [ ] Impliquer les représentants des collaborateurs/les RH
  - Préparer un accord avec l'organe de représentation des collaborateurs pour mettre en place la surveillance (si applicable dans votre juridiction)
  - Définir les exigences en matière de transparence
  - Préparer les informations destinées aux collaborateurs

1.2 Inventaire des données

- [ ] Lancer une Data discovery
  - Où sont stockées les données sensibles (serveurs de fichiers, SharePoint, espace de stockage sur le cloud, terminaux) ?
  - Quels types de données (données à caractère personnel, données financières, IP, données de santé) ?
  - Qui y a accès (créer une matrice d'autorisation) ?
  - Outils recommandés : outils automatisés pour la Data discovery (p. ex. Microsoft Purview, Varonis, BigID)
- [ ] Mappage du flux de données
  - Source des données → Traitement → Stockage → Transfert → Archivage/suppression
  - Identifier les vecteurs critiques (e-mails, téléversements sur le cloud, USB, imprimantes)
  - Visualisation : créer un diagramme du flux de données
- [ ] Évaluation du risque par catégorie de données

Catégorie de données	Sensibilité (1-5)	Volume	Accès/jour	Partagé à l'externe ?	Score du niveau de risque
Données client (données à caractère personnel)	5	Élevé	500	Oui	Critique
Données financières	5	Moyen	50	Rarement	Élevé
Code source	4	Élevé	200	Non	Élevé
Documents internes	2	Très élevé	2000	Oui	Moyen

2 Phase 2 : politique et classification (semaines 5 à 8)

2.1 Définir le schéma de classification des données

☐ Définir des niveaux de classification

Niveau	Définition	Exemples	Règle d'accès	Traitement
Public	À l'intention du public	Communiqués de presse, supports marketing	Aucune restriction	Pas de chiffrement requis
Interne	À usage interne	Plans de projet, notes de réunion	Réservé aux collaborateurs	Contrôle d'accès de base
Confidentiel	Critique pour l'entreprise	Contrats, prévisions financières, documents de fusion et acquisition	Principe du Need-to-know	Chiffrement + authentification multifacteur
À diffusion restreinte	Hautement sensible	Données du personnel, informations de paiement, dossiers de patients, secrets commerciaux	Autorisation explicite	Chiffrement + authentification multifacteur + piste d'audit + blocage DLP

☐ Mettre en place un processus d'étiquetage

- Classification automatique : reconnaissance des formes (numéros de carte de crédit, IBAN, etc.)
- Classification manuelle : formation des utilisateurs + rappels dans les applications Office
- Classification par défaut : nouveaux fichiers classés comme « interne » par défaut, jusqu'à leur évaluation

☐ Documenter la politique de classification

Modèle : directive de classification des données

1. Objectif

Cette politique définit la méthode de classification, l'étiquetage et la protection des données.

2. Portée

Tous les collaborateurs, sous-traitants et partenaires ayant accès aux données de l'entreprise.

3. Rôles

- Propriétaire des données : service, définit la classification
- Gardien des données : service informatique, installe les contrôles techniques
- Utilisateur des données : tous les collaborateurs ayant accès aux données, respectent les exigences en matière de traitement

4. Arbre de décision en matière de classification

Les données contiennent-elles des informations à caractère personnel ? → OUI → À diffusion restreinte
Leur divulgation causerait-elle du tort à l'entreprise ? → OUI → Confidentiel
Les données sont-elles prévues pour une utilisation en interne ? → OUI → Interne
NON → Public

5. Reclassification

Révision annuelle par le propriétaire des données. En cas de modification : mettre à jour l'étiquetage.

2.2 Créer une politique DLP

☐ Rédiger le document de politique

Modèle : politique de Data leak prevention

1. Objectif

Empêcher toute divulgation non autorisée des données sensibles de l'entreprise.

2. Portée

Tous les systèmes, réseaux, terminaux et services sur le cloud.

3. Actions interdites

- Transfert de données « à diffusion restreinte » ou « confidentielles » vers des adresses e-mail privées
- Téléversement de données sensibles vers des services sur le cloud non autorisés
- Copie de données sensibles vers des clés USB sans chiffrement
- Captures d'écran de documents « à diffusion restreinte » sans autorisation

4. Points de contrôle DLP

- Passerelle de messagerie (entrante/sortante)
- Proxy Web (téléversements sur le cloud)
- Agents de terminal (USB, presse-papiers, capture d'écran)
- Intégration d'une API cloud (Microsoft 365, Google Workspace, Slack)

5. Modes d'application

- Surveillance : journalisation uniquement, pas de blocage (phase pilote)
- Alerte : avertissement à l'utilisateur + équipe de sécurité
- Blocage : blocage automatique + ticket d'incident

6. Exceptions

Uniquement les exceptions ayant été approuvées par le RSSI, à condition d'être limitées dans le temps et documentées.

7. Réponse en cas d'incident

En cas de violation de données : ticket automatique → Évaluation dans les 4 heures → Transmission au service de sécurité si des données à diffusion restreinte sont affectées

8. Révision

Révision trimestrielle de la politique, après chaque incident.

☐ Créer une matrice du moindre privilège

Rôle	Données client	Données financières	Données RH	Code source	Documents marketing
Ventes	Lecture + Écriture	–	–	–	Lecture
Finance	–	Lecture + Écriture	–	–	–
RH	Lecture (noms /coordonnées)	–	Lecture + Écriture	–	–
Ingénierie	–	–	–	Lecture + Écriture	–
Marketing	Lecture (anonymisé)	–	–	–	Lecture + Écriture
Cadres	Lecture (tout)	Lecture (tout)	Lecture (tout)	Lecture (tout)	Lecture (tout)

☐ Définir la procédure de révision des accès

- Tous les trimestres : chaque responsable vérifie les droits d'accès de son équipe
- Si les postes évoluent : révocation automatique des anciens droits + demande de nouveaux droits
- En cas de départ : retrait immédiat de tous les droits d'accès

3 Phase 3 : Évaluation et choix des outils (semaines 9 à 12)

3.1 Liste des exigences

- [ ] Fonctionnalités indispensables
  - [ ] Prise en charge de tous les canaux de données (e-mail, Web, terminaux, cloud)
  - [ ] Inspection du contenu (reconnaissance des formes assistée par l'apprentissage automatique, OCR)
  - [ ] Intégration dans les systèmes existants (SIEM, SOAR, ticketing)
  - [ ] Intégration de chiffrement
  - [ ] Contrôle granulaire des politiques (par catégorie de données, groupe d'utilisateurs, action)
  - [ ] Rapports de conformité (RGPD, NIS2, ISO 27001)
  - [ ] Gestion des faux positifs (feedback aux utilisateurs, réglage de l'apprentissage automatique)
- [ ] Fonctionnalités souhaitables
  - [ ] Analyses comportementales (UEBA)
  - [ ] Analyse des données au repos (découverte)
  - [ ] Classification automatique
  - [ ] Flux de remédiation (p. ex., chiffrement automatique au lieu du blocage)
  - [ ] Libre-service pour les utilisateurs (demandes de déblocage)

3.2 Matrice d'évaluation des fournisseurs

- [ ] Créer une liste de présélection et l'évaluer

Critère	Pondération	Fournisseur A	Fournisseur B	Fournisseur C
Fonctionnalité				
DLP pour e-mails	15 %	9/10	8/10	7/10
Cloud DLP (API)	20 %	8/10	9/10	6/10
DLP pour terminaux	15 %	7/10	9/10	8/10
Apprentissage automatique/analyse comportementale	10 %	9/10	7/10	5/10
Intégration				
SIEM/SOAR	10 %	8/10	8/10	9/10

Critère	Pondération	Fournisseur A	Fournisseur B	Fournisseur C
Stack technique existante	5 %	7/10	9/10	6/10
Ergonomie				
Interface utilisateur pour admin	5 %	8/10	7/10	9/10
Gestion des faux positifs	10 %	9/10	8/10	7/10
Coût				
Prix de la licence	5 %	7/10	8/10	9/10
Effort d'implémentation	5 %	8/10	7/10	8/10
Score global	100 %	8,2	8,1	7,3

- [ ] Faire un POC
  - Durée du test : 4 semaines
  - Portée du test : e-mail + cloud + 50 terminaux de test
  - Critères de réussite : <5 % de faux positifs, <100 ms de latence, plus de 95 % de taux de détection

4 Phase 4 : implémentation (semaines 13 à 20)

4.1 Implémentation technique

- [ ] DLP pour e-mails
  - Ajustement de l'enregistrement MX ou configuration du relais SMTP
  - Règles de politique : analyse sortante pour les données à diffusion restreinte/confidentielles
  - Configuration de la boîte e-mail de mise en quarantaine
  - Procédure de transmission à l'échelon supérieur : équipe de sécurité + responsable en cas de blocage
- [ ] Web/Cloud DLP
  - Intégration du proxy ou du CASB
  - Activation de l'inspection SSL (attention : implications de la protection des données)
  - Connecteurs API : Microsoft 365, Google Workspace, Slack, Salesforce
  - Politique : blocage du téléversement des données à diffusion restreinte vers des services sur le cloud non approuvés
- [ ] DLP pour terminaux
  - Déploiement de l'agent (étape par étape : service informatique → groupe pilote → déploiement complet)
  - Blocage des clés USB pour les données à diffusion restreinte (liste blanche pour les clés USB chiffrées)
  - Contrôle du presse-papiers, prévention des captures d'écran
  - Mode hors ligne : application de la politique même sans connexion réseau
- [ ] Intégration de la gestion des incidents
  - Intégration SIEM : alertes DLP → corrélation avec d'autres événements de sécurité
  - Ticketing : automatisation des tickets en cas de violations de données très graves
  - Playbooks SOAR : suspension automatique du compte en cas de violations de données critiques

4.2 Plan de déploiement

- [ ] Phase pilote (semaines 13 à 16)
  - Groupe cible : service informatique (20 à 50 utilisateurs)
  - Mode : surveillance uniquement

- Objectif : définir une ligne de référence, déterminer le taux de faux positifs, affiner les politiques

☐ Déploiement par phases (semaines 17 à 20)

- Semaine 17 : Finance (mode alerte)
- Semaine 18 : RH + service juridique (mode alerte)
- Semaine 19 : Ingénierie + ventes (mode alerte)
- Semaine 20 : Reste de l'entreprise (mode alerte)

☐ Phase d'application (à partir de la semaine 21)

- Transition progressive vers le mode blocage
- Commencer par les données à diffusion restreinte
- Au bout de 2 semaines : ajouter les données confidentielles

5 Phase 5 : Gestion du risque humain (en parallèle de la phase 4)

5.1 Campagne de sensibilisation

- [ ] Plan de communication
  - Semaine 12 : annonce par le PDG/RSSI (réunion plénière)
  - Semaines 13 à 16 : groupe pilote : formation intensive + séances de questions-réponses
  - Semaines 17 à 20 : communication autour du déploiement : article sur l'Intranet, e-mail, briefings des responsables
  - À partir de la semaine 21 : rappels continus (newsletter mensuelle)
- [ ] Développer des modules de formation
  1. Module 1 : Pourquoi la DLP ? (5 min)
     - Risques de violations de données (exemples de cas)
     - Obligations légales (RGPD, NIS2)
     - Responsabilité personnelle
  2. Module 2 : Classification des données (10 min)
     - Niveaux et exemples
     - Comment bien classifier les données ?
     - Exercice pratique : classifier 5 exemples de documents
  3. Module 3 : Qu'ai-je le droit de faire (et de ne pas faire) ? (10 min)
     - À faire et ne pas faire
     - Que se passe-t-il en cas de violation de données ?
     - Comment demander des exceptions ?
  4. Module 4 : Phishing et ingénierie sociale (15 min)
     - Détecter les e-mails de phishing
     - Scénarios de fraude au président
     - Processus de signalement
- [ ] Simulations de phishing
  - Fréquence : mensuelle, aléatoire
  - Alternance des modèles : fraude au président, fausse facture, phishing des identifiants de connexion, malware en pièce jointe
  - Suivi : en cas de clic → page de micro-apprentissage apparaissant immédiatement (3 min)
  - Gamification : tableau de classement (anonymisé), badges pour les personnes qui ont signalé

5.2 Tableau de bord du risque humain

☐ Définir et suivre les KPI

KPI	Valeur cible	Méthode de mesure
Taux de clics sur des tentatives de phishing	<5 %	Outil de simulation de phishing
Taux de signalement (e-mails suspects)	>30 %	Analyse des données du bouton d'alerte phishing
Taux d'achèvement de la formation	>95 %	Rapports du LMS
Violations de la DLP pour 1 000 utilisateurs	<10/mois	Journaux du système DLP
Récidives de violations (par le même utilisateur)	<2 %	Analyse des données du système DLP
Human Security Index	>75/100	Tableau de bord de gestion du risque humain

6 Phase 6 : Conformité et documentation (semaines 21 à 24)

[LOCAL PART]

6.1 Mappage de la conformité

Le mappage suivant prend les cadres réglementaires européens (RGPD, NIS2, ISO 27001) comme exemple de travail. Adaptez les références d'articles, les délais et les autorités en fonction des cadres réglementaires qui s'appliquent à votre juridiction.

☐ Tenir compte des exigences du RGPD

Articles du RGPD	Exigence	Mesure DLP	Statut
Art. 5 (1f)	Intégrité et confidentialité	Politiques DLP + chiffrement	☐
Art. 25	Privacy-by-design	Classification « Interne » par défaut	☐
Art. 32	Mesures techniques	DLP + Contrôle des accès + Surveillance	☐
Art. 33	Obligation de notification (72 heures)	Intégration de la réponse en cas d'incidents	☐
Art. 35	DPIA	DPIA menée pour le suivi de la DLP	☐

☐ Tenir compte des exigences de la directive NIS2 et du Référentiel Cyber France (version de travail)

Articles de la directive NIS2	Exigence	Mesure DLP	Statut
Objectif de sécurité 2 (ReCyF)/Art. 21	Gestion du risque de cybersécurité	DLP dans le cadre de la stratégie de gestion du risque	☐
Objectif de sécurité 3 (ReCyF)/Art. 23	Obligation de notification (alerte précoce dans les 24 heures)	Alertes automatiques + transmission à l'échelon supérieur	☐
Objectif de sécurité 17 (ReCyF)/Art. 32	Audit et documentation	Journaux DLP, documents de politique, pistes d'audit	☐

☐ Tenir compte de l'annexe A 8.12 de la norme ISO 27001:2022

- Data leakage prevention documentée comme mesure de contrôle

- Description de la procédure : comment l'entreprise prévient-elle l'exfiltration des données ?
- Documents d'aide : politique DLP, configuration de l'outil, journaux, signalement des incidents

6.2 Documentation

- [ ] Créer des documents obligatoires
  - [ ] Politique DLP (voir le modèle ci-dessus)
  - [ ] Politique de classification des données
  - [ ] Plan de réponse en cas d'incidents (voir ci-dessous)
  - [ ] Accord d'exploitation (surveillance)
  - [ ] Analyse d'impact relative à la protection des données (DPIA)
  - [ ] Manuel de l'administrateur (système DLP)
  - [ ] Guide de l'utilisateur (classification des données, procédure pour les exceptions)

7 Phase 7 : Réponse en cas d'incident (continue)

7.1 Plan de réponse en cas d'incident

Modèle : Playbook de réponse en cas d'incident DLP

Phase 1 : Détection (0 à 15 min)

- [ ] Réception d'une alerte DLP (e-mail, SIEM, ticket)
- [ ] Classification de la gravité :
  - Critique : données à diffusion restreinte + accès externe + gros volume
  - Élevée : données confidentielles + accès externe
  - Intermédiaire : données confidentielles + accès interne
  - Faible : données internes + comportement inhabituel
- [ ] Affectation de l'ingénieur d'astreinte

Phase 2 : Confinement (15 à 60 min)

- [ ] En cas de gravité critique/élevée : prise de mesures immédiates
  - Verrouillage du compte concerné
  - Rappel de l'e-mail depuis la boîte d'envoi du destinataire (si c'est encore possible)
  - Déconnexion du terminal du réseau (si exfiltration active)
- [ ] Création d'un instantané pour l'analyse forensique (journaux, vidage de la mémoire, image disque)
- [ ] Communication des informations au responsable en cas d'incidents (RSSI ou adjoint)

Phase 3 : Évaluation (1 à 4 heures)

- [ ] Évaluation des données :
  - Quelles données ? (classification, volume, nombre de personnes affectées)
  - Où ? (destinataire interne/externe, domaine, service sur le cloud)
  - Comment ? (e-mail, USB, téléversement cloud, capture d'écran)
  - Pourquoi ? (erreur, ingénierie sociale, intention malveillante)
- [ ] Entretien avec l'utilisateur (si disponible, sauf en cas de suspicion d'intention malveillante)
- [ ] Évaluation juridique : obligation de notification en vertu de la loi applicable sur la protection des données et la cybersécurité ? [LOCAL PART - EU example below]
  - Art. 33 du RGPD : notification à la CNIL dans les 72 heures ?

- Art. 23 de la directive NIS2 : notification initiale à l'ANSSI/CERT-FR sans délai (souvent une alerte précoce sous 24h et une notification circonstanciée sous 72h pour les secteurs critiques) ?
- Informer les personnes concernées ? (art. 34 du RGPD)

☐ Décision : faire remonter à la direction/au service juridique ?

Phase 4 : Notification (dans les délais légaux)

☐ Signalement en interne : signalement de l'incident au RSSI, au service juridique, délégué à la protection des données

☐ Signalement à l'externe (si nécessaire) : [LOCAL PART - EU example below]

- RGPD : notification à la CNIL (formulaire)
- NIS2 : signalement initial à l'ANSSI/CERT-FR
- Personnes concernées : e-mail/courrier avec les détails + conseils de mesures à prendre

☐ Documentation : mise à jour du ticket de l'incident (délais, mesures, communication)

Phase 5 : Suivi (en l'espace de 1 semaine)

☐ Analyse des causes premières :

- Cause technique (lacune dans la politique, faux négatif)
- Cause humaine (négligence, manque de formation, intention malveillante)

☐ Remédiation :

- Ajustement de la politique
- Contrôles supplémentaires (p. ex. principe des quatre yeux pour les données sensibles)
- Nouvelle formation des utilisateurs (ciblée ou large)
- Mesures disciplinaires (si intention malveillante)

☐ Enseignements tirés : Documentation + Présentation à l'équipe de sécurité

☐ Mise à jour de la politique/du playbook

Phase 6 : Révision (trimestrielle)

☐ Passer en revue tous les incidents : Schémas ? Récidivistes ? Vulnérabilités ?

☐ Rapport avec les KPI pour la direction

7.2 Matrice de transmission à l'échelon supérieur

Gravité	Délai de réponse	Qui est informé ?	Mesures
Critique	<15 min	RSSI, service juridique, PDG, délégué à la protection des données	Blocage du compte, analyse forensique, contrôle du rapport externe

Gravité	Délai de réponse	Qui est informé ?	Mesures
Forte	<1 heure	RSSI, équipe de sécurité, gestionnaire des utilisateurs	Verrouillage temporaire du compte, entretien avec l'utilisateur, révision de la politique
Intermédiaire	<4 heures	Équipe de sécurité, gestionnaire des utilisateurs	Avertissement à l'utilisateur, nouvelle formation, renforcement de la surveillance
Faible	<24 heures	Équipe de sécurité	Journalisation, en cas de récidive → Intermédiaire

8 Phase 8 : KPI et rapport (en continu)

8.1 Tableau de bord des KPI DLP

☐ Indicateurs techniques

KPI	Formule	Cible	Intervalle de détection
Taux de détection	(violations de données détectées/ensemble des violations) × 100	>95 %	Mensuel (test avec des données factices)
Taux de faux positifs	(Faux positifs/ensemble des alertes) × 100	<5 %	Hebdomadaire
Canaux concernés par la politique	(canaux de données concernés/ensemble des canaux de données) × 100	100 %	Trimestriel
MTTR (temps moyen de réponse)	Temps moyen qui s'écoule entre l'alerte et le confinement	<1 heure (critique)	Par incident
Temps de disponibilité du système	Disponibilité du système DLP	>99,5 %	Mensuel

☐ Indicateurs de conformité

KPI	Description	Valeur cible	Rapports
Violations pour 1 000 utilisateurs	Nombre de violations DLP normalisées	<10/mois	Mensuel
Récidivistes	Utilisateurs avec >2 violations en 3 mois	<2 % des utilisateurs	Trimestriel
Signalement des incidents (RGPD/NIS2)	Nombre d'incidents à signaler	0 (cible)	Annuel
Résultats de l'audit	Résultats des audits internes/externes	0 Critique/Élevé	Après l'audit
Taux de conformité des politiques	Pourcentage d'utilisateurs ayant terminé la formation sur la politique	>95 %	Trimestriel

☐ Indicateurs de risque humain

KPI	Description	Valeur cible	Outil
Human Security Index	Indicateur de sécurité agrégé	>75/100	Tableau de bord du risque humain
Taux de clic sur des tentatives de phishing	% des utilisateurs qui cliquent sur les simulations	<5 %	Outil de simulation de phishing
Taux d'alerte phishing	% des utilisateurs qui signalent les e-mails suspects	>30 %	Analyse des données du bouton d'alerte
Achèvement de la formation	% des utilisateurs ayant terminé la formation sur la DLP	>95 %	LMS
Score de sensibilisation	Résultats au quiz après la formation	>80 % de bonnes réponses	LMS

8.2 Rapports à la direction

- [ ] Rapport mensuel (1 page)
  - Nombre de violations (tendance)
  - Top 3 des types de violation
  - Incidents de gravité critique/élevée (détails)
  - Taux de faux positifs
  - Actions en cours
- [ ] Synthèse trimestrielle
  - Tableau de bord des KPI (visuel)
  - Statut de conformité (RGPD, NIS2, ISO 27001)
  - Calcul du retour sur investissement (dommages et amendes évités)
  - Enseignements tirés des incidents
  - Feuille de route pour le prochain trimestre

9 Phase 9 : Amélioration continue (en cours)

9.1 Cycles d'analyse

- [ ] Hebdomadaire (équipe de sécurité)
  - Analyse des nouveaux faux positifs et ajustement des politiques
  - Révision des violations critiques
  - Performance de l'outil (temps de disponibilité, latence)
- [ ] Mensuel (équipe de sécurité + opérations informatiques)
  - Analyse des KPI
  - Évaluation des retours des utilisateurs
  - Ajustements de la politique
- [ ] Trimestriel (RSSI + direction)
  - Analyse stratégique : Avons-nous atteint nos objectifs ?
  - Analyse budgétaire : Faut-il d'autres outils/ressources ?
  - Contrôle de la conformité : Avons-nous satisfait à toutes les exigences ?
  - Enseignements tirés de tous les incidents
- [ ] Annuel (audit complet)
  - Test de pénétration externe (incluant des scénarios d'exfiltration de données)
  - Analyse de la politique : Tous les éléments sont-ils encore à jour ?
  - Évaluation de l'outil : Existe-t-il de meilleures options ?
  - Accord d'exploitation : Des modifications sont-elles nécessaires ?

9.2 Cycles de feedback

- [ ] Canaux pour le feedback des utilisateurs
  - Formulaire : « Le blocage DLP était injustifié/justifié »
  - Évaluation : faux positifs → ajustement de la politique
  - Réponse : l'utilisateur reçoit un feedback dans les 24 heures
- [ ] Programme de champions de sécurité
  - 1 champion par département (bénévole)
  - Réunion mensuelle : feedback, nouvelles menaces, cas pratiques
  - Les champions forment leurs équipes (multiplicateurs)

Outils et modèles

Modèle 1 : ticket de réponse en cas d'incident

ID de l'incident : DLP-2026-001

Date/heure : [AAAA-MM-JJ, HH:MM, fuseau horaire]

Sévérité : [Critique / élevée / intermédiaire / faible]

Statut : [Nouveau / En progrès / Confiné / Résolu / Clôturé]

DÉTECTION

Source de l'alerte : [Système DLP / SIEM / Rapport utilisateur]

Utilisateur concerné : [Nom, service, e-mail]

Détails des données :

- Classification : [Public / Interne / Confidentiel / À diffusion restreinte]
- Type de données : [données à caractère personnel / Données financières / IP / Autre]
- Volume : [Nombre de fichiers / Dossiers de données / Mo]

Canal : [E-mail / Cloud / USB / Imprimante / Autre]

Destination : [Interne / Externe : Domaine/Service]

CONFINEMENT

Mesures :

- ☐ Compte bloqué (horodatage : _____)
- ☐ E-mail rappelé (oui/non)
- ☐ Terminal isolé
- ☐ Instantané créé pour l'analyse forensique

ÉVALUATION

Cause première : [Technique / Erreur humaine / Ingénierie sociale / Intention malveillante]

Obligation de notification : [PARTIE LOCALE - à adapter à la loi en vigueur]

- ☐ art. 33 du RGPD (CNIL)
- ☐ Art. 34 du RGPD (Personnes concernées)
- ☐ Art. 23 de la directive NIS2 (ANSSI)
- ☐ Aucune obligation de notification (raison : _____)

SUIVI

Ajustements de la politique : [Description]

Mesures auprès des utilisateurs : [Nouvelle formation / Avertissement / Mesure disciplinaire / Aucune]

Enseignements tirés : [Résumé]

Modèle 2 : Demande d'exception à la politique

Personne à l'origine de la demande : [Nom, Service]

Date : [AAAA-MM-JJ]

Justification commerciale : [Pourquoi l'exception est-elle nécessaire ?]

Règle de la politique concernée : [p. ex. « Blocage de la clé USB pour les données à divulgation restreinte »]

Données concernées : [Classification, description]

Durée de l'exception : [Durée limitée jusqu'au AAAA-MM-JJ / Illimitée]

Mesures compensatoires : [p. ex. « USB cryptée », « Principe du double contrôle »]

Approbation :

- ☐ Approuvé par : [RSSI / Adjoint]
- ☐ Refusé (Raison : _____)

Modèle 3 : Ordre du jour de l'analyse trimestrielle de la DLP

1. Analyse des KPI (15 min)
   - Taux de détection, taux de faux positifs, tendance des violations
   - Mesures prises au dernier trimestre : statut ?
2. Analyse des incidents (20 min)
   - Tous les incidents de gravité critique/élevée : schémas ?
   - Les enseignements qui ont été tirés ont-ils été mis en pratique ?
3. Statut de conformité (10 min) [LOCAL PART]
   - RGPD : Toutes les exigences ont-elles été satisfaites ?
   - NIS2 : Procédures de signalement testées ?
   - ISO 27001 : préparation à l'audit effectué ?
4. Feedback à l'utilisateur (10 min)
   - Faux positifs les plus fréquents → Ajustement de la politique
   - Retour au champion
5. Feuille de route (15 min)
   - Nouvelles exigences (nouveaux outils sur le cloud, nouveaux types de données)
   - Optimisation de l'outil

- Budget pour le prochain trimestre

6. Mesures prises (10 min)
   - Qui fait quoi et quand ?

Annexe : glossaire et références

Glossaire

- **CASB (Cloud Access Security Broker) :** couche de contrôle entre les utilisateurs et les services sur le cloud
- **DLP (Data Leak Prevention) :** technologie de prévention contre les divulgations de données non autorisées
- **DPIA (Data Protection Impact Assessment) :** analyse obligatoire du traitement des données à haut risque (art. 35 du RGPD)
- **Faux positif :** fausse alarme (la DLP a bloqué une action inoffensive)
- **MTTR (Mean Time to Respond) :** temps moyen de réponse en cas d'incident
- **PII (Personally Identifiable Information) :** données à caractère personnel
- **SIEM (Security Information and Event Management) :** outil de journalisation et de corrélation centralisé
- **SOAR (Security Orchestration, Automation and Response) :** automatisation des flux de sécurité
- **UEBA (User and Entity Behaviour Analytics) :** détection des anomalies dans les comportements des utilisateurs

Références réglementaires [LOCAL PART]

- **RGPD (UE 2016/679) :** https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679
- **Directive NIS2 (UE 2022/2555) :** https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2555 – ReCyF (version de travail) http://messervicescyber-ressources.cellar-c2.services.clever-cloud.com/20260317_NIS_V2_ReCyF_v2.5.pdf
- **ISO/CEI 27001:2022 :** https://www.iso.org/fr/standard/27001