silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Plan d'action

Mise en conformité avec la Directive NIS 2

Mars 2025

Mise en conformité à la Directive NIS 2 - Plan d'action opérationnel

L'entrée en vigueur de la directive NIS 2 impose aux organisations concernées un renforcement de leur gouvernance et de leur posture en matière de cybersécurité. Cette mise en conformité nécessite une approche méthodique et rigoureuse. Le présent plan d'action détaille chaque étape de cette mise en conformité, avec un focus sur les **objectifs** à atteindre et les **actions concrètes** à mettre en place.

Table des matières

Étape 1 : Évaluation approfondie du périmètre d'application et identification précise du statut (EE ou EI)

Contexte

La première étape est fondamentale car elle détermine l'ensemble des obligations auxquelles votre organisation sera soumise. Une mauvaise identification pourrait entraîner une non-conformité coûteuse ou une application inutile de mesures trop strictes ou insuffisantes. La directive NIS 2 étend considérablement le champ d'application de NIS 1, passant d'une liste limitée d'Opérateurs de Services Essentiels (OSE) et de Fournisseurs de Services Numériques (FSN) à un éventail plus large d'entités essentielles (EE) et d'entités importantes (EI) opérant dans 18 secteurs d'activités. Ces secteurs sont classés en hautement critiques et critiques. Contrairement à NIS 1 où les États désignaient les entités, NIS 2 implique une responsabilité accrue pour les entreprises et organisations de se déclarer auprès des autorités. De plus, au-delà des seuils quantitatifs (taille, chiffre d'affaires), la criticité de l'activité au sein d'un secteur peut modifier l'application de la directive. Il est également crucial de considérer l'effet cascade sur les prestataires critiques des EE et EI. Les entités recensées comme critiques au sens de la directive (UE) 2022/2557 (REC) doivent obligatoirement être désignées comme entités essentielles au sens de NIS 2.

Actions

Identification du périmètre et du secteur d'activité

- ☐ Recenser l'ensemble des activités exercées par l'organisation.
- ☐ Vérifier si l'activité principale ou des services secondaires appartiennent aux **secteurs hautement critiques** (Annexe I de NIS 2) ou aux **secteurs critiques** (Annexe II de NIS 2).
- ☐ Consulter les ressources officielles (ANSSI, ENISA, textes réglementaires) pour affiner cette classification.

Évaluation de la taille de l'organisation

- ☐ Recueillir et analyser les **effectifs**, le **chiffre d'affaires annuel** et le **total du bilan**.
- ☐ Comparer ces valeurs aux seuils d'éligibilité :
  - Entité Essentielle (EE) : +250 salariés et CA > 50M€ ou bilan > 43M€.
  - Entité Importante (EI) : 50-249 salariés et CA entre 10M€ et 50M€ ou bilan entre 10M€ et 43M€.
- ☐ Vérifier si des précisions ont été apportées par décret en France.

Analyse de la criticité des services

- ☐ Identifier les services fournis et leur impact potentiel en cas d'interruption sur :
  - L'économie (perturbation des transactions, infrastructures stratégiques).
  - La sécurité publique (accès aux services d'urgence, transport).
  - La santé (hôpitaux, services médicaux critiques).
- ☐ Déterminer si l'organisation doit être classée comme **EE ou EI** même en deçà des seuils de taille, en raison de la nature essentielle de ses services.

Identification des exemptions

- ☐ Vérifier si l'organisation entre **automatiquement dans le champ de NIS 2** (ex. fournisseurs de réseaux, services publics locaux, prestataires de services de confiance).
- ☐ Vérifier si elle est **exclue** en raison d'activités liées à la sécurité nationale, la défense ou l'application de la loi.

Cartographie des dépendances critiques

- ☐ Recenser les **fournisseurs et prestataires de services** intervenant dans la gestion des systèmes d'information, la sécurité informatique ou d'autres activités critiques.
- ☐ Vérifier si ces prestataires sont eux-mêmes soumis à NIS 2 en raison de leur rôle stratégique.

Consultation des ressources de l'ANSSI

- ☐ Utiliser le portail **"Mon Espace NIS 2"** pour déterminer si l'organisation est concernée et sous quelle catégorie.
- ☐ Suivre les évolutions de la transposition en droit français et les critères d'identification nationaux.

Documentation de l'évaluation

- ☐ Archiver les informations collectées sur :
  - Le secteur d'activité.
  - La taille et les seuils financiers.
  - La criticité des services et les risques associés.
  - Les dépendances avec les fournisseurs.
- ☐ Préparer la documentation en vue d'une **déclaration auprès des autorités compétentes** avant la date limite (potentiellement le 17 janvier pour la déclaration volontaire, le 17 avril 2025 pour la déclaration nationale des États membres).

Résultat attendu

Une vision claire du statut de l'organisation vis-à-vis de la directive **NIS 2**, permettant d'anticiper ses obligations et d'adapter son plan d'action.

Étape 2 : Constitution d'une équipe projet pluridisciplinaire et obtention d'un engagement fort de la direction

Contexte

La mise en œuvre réussie de la directive NIS 2 repose intrinsèquement sur un engagement indéfectible de la direction et la mise en place d'une équipe projet compétente et

représentative des différentes fonctions de l'organisation. La direction ne doit pas considérer la cybersécurité comme une simple affaire informatique, mais comme une fonction métier stratégique ayant un impact direct sur la pérennité et la croissance de l'entreprise. Les cadres supérieurs seront directement responsables de la sécurité au sein de leur organisation et peuvent même faire l'objet d'une interdiction temporaire d'exercer en cas de négligence entraînant une atteinte grave à la sécurité. Il est donc crucial que les dirigeants soient formés spécifiquement à la mise en conformité NIS 2, aux normes de sécurité informatique et à la gestion des risques pour prendre des décisions éclairées. En présentant la conformité non seulement comme une obligation légale mais aussi comme une opportunité d'améliorer la résilience opérationnelle et de favoriser une transformation numérique sécurisée, le *Responsable de la Sécurité des Systèmes d'Information* (RSSI) peut obtenir l'adhésion et le soutien nécessaires de la direction.

Actions

Désignation du responsable de projet NIS 2

- ☐ **Identifier et nommer un responsable de projet** chargé de piloter l'ensemble de la démarche de mise en conformité.
- ☐ Sélectionner une personne disposant :
  - D'une expertise en cybersécurité et gestion des risques.
  - D'une expérience en gestion de projets complexes.
  - De compétences en communication pour interagir avec la direction et les équipes opérationnelles.
- ☐ Confirmer son rôle et ses responsabilités via une **lettre de mission** validée par la direction.

Constitution d'une équipe projet pluridisciplinaire

- ☐ **Créer une équipe projet représentative** en intégrant des experts des domaines suivants :
  - IT et cybersécurité : mise en œuvre des mesures techniques et opérationnelles.
  - Juridique et conformité : analyse des obligations réglementaires et élaboration des politiques.
  - Ressources humaines : formation, sensibilisation, gestion des accès et du personnel.
  - Opérations métiers : identification des actifs critiques et évaluation des impacts opérationnels.
  - Direction générale : allocation des ressources et validation stratégique.
- ☐ **Intégrer les partenaires externes stratégiques** (fournisseurs, sous-traitants, consultants) pour garantir la conformité de la chaîne d'approvisionnement.

Obtenir un engagement fort de la direction

- ☐ **Organiser une réunion dédiée avec la direction** pour :
  - Présenter la directive NIS 2, ses exigences et ses impacts concrets sur l'organisation.
  - Expliquer les risques de non-conformité (sanctions financières, responsabilité personnelle des dirigeants, impacts réputationnels).

- Mettre en avant les bénéfices stratégiques : renforcement de la résilience, opportunités commerciales, conformité anticipée aux réglementations futures.
- Illustrer le propos avec des cas concrets d'attaques cyber et leurs conséquences.
- Obtenir une validation de la stratégie et des ressources nécessaires (budget, personnel, outils).

Renforcer l'adhésion des dirigeants via la formation

- ☐ **Identifier et mettre en place un programme de formation spécifique pour la direction** :
  - Principes de cybersécurité et gestion des risques.
  - Obligations de NIS 2 et responsabilités légales des cadres dirigeants.
  - Prise de décision stratégique en matière de cybersécurité.
- ☐ **Planifier des mises à jour régulières** pour suivre l'évolution des menaces et des réglementations.

Formaliser et documenter l'engagement de la direction

- ☐ **Rédiger et signer une charte de projet** incluant :
  - Les objectifs de conformité à NIS 2.
  - Les rôles et responsabilités de l'équipe projet.
  - L'engagement de la direction en termes de ressources et de suivi.
- ☐ **Archiver les comptes rendus des réunions stratégiques** pour démontrer l'implication de la direction en cas de contrôle.

Résultat attendu

Une gouvernance claire et un soutien fort de la direction, garantissant une mise en conformité efficace et durable avec **NIS 2**.

Étape 3 : Réalisation d'un audit initial approfondi de cybersécurité et analyse rigoureuse des écarts

Contexte

Avant d'initier la mise en œuvre de mesures correctives, il est impératif de réaliser un audit exhaustif de la posture de cybersécurité actuelle de votre organisation. Cet audit initial constitue un état des lieux précis de vos dispositifs de sécurité existants et permet d'identifier les vulnérabilités de vos systèmes ainsi que les domaines de non-conformité potentiels avec les exigences de la directive NIS 2. Une analyse des écarts méthodique doit ensuite être menée en comparant les conclusions de cet audit aux obligations spécifiques de NIS 2 qui s'appliquent à votre catégorie d'entité, qu'elle soit Essentielle (EE) ou Importante (EI). La

gestion des risques étant au cœur de la directive NIS 2, cet audit et cette analyse doivent être orientés vers l'identification et la priorisation des risques cyber auxquels votre organisation est exposée.

Actions

Préparation et cadrage de l'audit

- ☐ **Définir les objectifs de l'audit** : établir un état des lieux précis de la cybersécurité et identifier les écarts avec les exigences de **NIS 2**.
- ☐ **Déterminer le périmètre de l'audit** : inclure l'ensemble des actifs, des processus et des parties prenantes concernés.
- ☐ **Désigner une équipe d'audit** composée des services **IT, sécurité, juridique, conformité et métiers**.
- ☐ **Envisager l'intervention d'un prestataire externe** pour bénéficier d'une expertise objective (ex. audit certifié ISO 27001).

Réalisation de l'audit initial

- ☐ **Cartographier et inventorier les systèmes d'information critiques** :
  - Identifier les **actifs clés** et leur rôle dans les activités essentielles.
  - Évaluer la **sensibilité des données** manipulées et leur niveau de protection.
- ☐ **Évaluer les politiques et procédures de sécurité existantes** :
  - Vérifier leur cohérence avec les standards de cybersécurité et leur mise en application effective.
  - Examiner l'existence d'une gouvernance de la sécurité et de mécanismes de contrôle internes.
- ☐ **Analyser les mesures techniques de cybersécurité** :
  - Évaluer les pare-feu, systèmes de détection d'intrusion, antivirus, solutions de chiffrement et authentification.
  - Vérifier la présence de mesures de protection contre les menaces avancées.
- ☐ **Examiner les processus de gestion des incidents** :
  - Vérifier la capacité de l'organisation à détecter, répondre et récupérer après un incident.
  - Évaluer les mécanismes de signalement et d'escalade en cas de crise cyber.
- ☐ **Auditer les plans de continuité et de reprise après sinistre (PCA/PRA)** :
  - Vérifier la présence d'un PCA/PRA formalisé, testé et mis à jour régulièrement.
  - Évaluer les délais de reprise (RTO) et points de reprise (RPO) en cas d'incident majeur.
- ☐ **Évaluer la sécurité de la chaîne d'approvisionnement** :
  - Recenser les fournisseurs et prestataires critiques pour l'organisation.
  - Vérifier leur niveau de conformité et leurs engagements contractuels en matière de cybersécurité.

Analyse des écarts avec les exigences de NIS 2

- ☐ **Comparer les résultats de l'audit aux obligations de NIS 2** applicables au statut de l'organisation (**EE ou EI**).
- ☐ **Examiner chaque exigence réglementaire** et identifier les non-conformités.
- ☐ **Documenter chaque écart** de manière détaillée, en précisant :
    - L'obligation NIS 2 concernée.
    - La situation actuelle et la vulnérabilité identifiée.
    - L'impact potentiel sur la sécurité et la conformité.

Priorisation des écarts et recommandations

- ☐ **Évaluer la criticité des écarts** en tenant compte :
    - De l'impact potentiel sur la sécurité et la continuité des services.
    - De la probabilité d'occurrence des risques identifiés.
- ☐ **Élaborer une matrice de risques** pour organiser les actions correctives selon leur priorité :
    - Écarts critiques → correction immédiate (ex. absence de gestion des incidents).
    - Écarts modérés → planification à court terme.
    - Écarts mineurs → intégration dans une stratégie d'amélioration continue.

Documentation et restitution des résultats

- ☐ **Rédiger un rapport d'audit détaillé**, incluant :
    - L'inventaire des actifs et leur niveau de protection.
    - Les écarts identifiés et leur criticité.
    - Les recommandations d'actions correctives.
- ☐ **Présenter les résultats à la direction** pour obtenir une validation des priorités et un engagement sur les moyens nécessaires.

Résultat attendu :

Une cartographie claire des vulnérabilités et un plan d'actions priorisé pour aligner l'organisation avec les exigences de NIS 2.

Étape 4 : Élaboration du plan de conformité détaillé, du plan de résilience et du budget prévisionnel

Contexte

Suite à l'analyse approfondie des écarts, l'étape cruciale suivante consiste à élaborer un plan de conformité détaillé et un plan de résilience, décrivant précisément les actions à entreprendre pour satisfaire aux exigences de la directive NIS 2, en y intégrant des échéances réalistes, l'identification des responsables pour chaque tâche, ainsi que l'ensemble des ressources nécessaires. Parallèlement, l'établissement d'un budget prévisionnel précis et justifié est indispensable pour obtenir l'approbation et l'allocation des ressources par la direction. Ce plan de conformité doit être perçu comme une feuille de route dynamique, susceptible d'évoluer en fonction des retours d'expérience et des directives de l'ANSSI. La gestion des risques identifiée lors de l'étape précédente doit être au cœur de ce plan, guidant la priorisation des actions et l'allocation des ressources. Il est également important de noter que pour les Opérateurs d'Importance Vitale (OIV), le plan de sécurité opérateur (PSO) et le plan de continuité d'activité (PCA) sont fusionnés en un plan de résilience opérateur (PRO) unique, qui détaillera les mesures de résilience basées sur une analyse des risques et approuvé par l'autorité administrative dans un délai de dix mois suivant leur désignation. Ce plan, ainsi que les plans particuliers de protection (PPP), devront être revus au moins tous les quatre ans.

Actions

Définition des objectifs et de la feuille de route

- ☐ **Fixer des objectifs SMART** (Spécifiques, Mesurables, Atteignables, Réalistes, Temporellement définis) pour la mise en conformité NIS 2.
- ☐ **Établir une feuille de route détaillée** en listant :
  - Les tâches à réaliser pour combler les écarts identifiés lors de l'audit.
  - L'ordre de priorité en fonction de la criticité des risques et de l'effort requis.
  - Les dépendances entre tâches et les délais de réalisation réalistes.
- ☐ **Structurer la mise en œuvre** en trois phases :
  - Évaluation et planification (3 à 6 mois).
  - Déploiement des mesures correctives (6 à 12 mois).
  - Suivi et ajustement continu (audit régulier et amélioration).

Attribution des responsabilités et mobilisation des ressources

- ☐ **Désigner un responsable de projet NIS 2** chargé de superviser la mise en conformité et le suivi de l'avancement.
- ☐ **Attribuer des responsabilités précises** aux membres de l'équipe projet pluridisciplinaire (IT, juridique, conformité, RH, métiers, direction).
- ☐ **Recenser les ressources nécessaires** :
  - Humaines : compétences internes, formation des équipes.
  - Financières : budget pour équipements, formations, conseil externe.
  - Techniques : outils de cybersécurité, infrastructures sécurisées.
  - Externes : consultants spécialisés, auditeurs.

- ☐ **Évaluer la nécessité d'une assistance externe** (ex. audit de conformité, support technique pour PME).

Élaboration d'un budget prévisionnel détaillé

- ☐ **Évaluer les coûts des actions nécessaires**, incluant :
    - Audit initial et suivi.
    - Acquisition ou mise à niveau des outils et solutions de cybersécurité.
    - Programmes de formation et sensibilisation du personnel et de la direction.
    - Recours à des consultants spécialisés et experts en conformité.
    - Coût des infrastructures informatiques sécurisées (serveurs, cloud, SIEM, pare-feu).
- ☐ **Intégrer une marge pour imprévus** (10 à 15% du budget total).
- ☐ **Explorer les aides financières disponibles** auprès de l'État ou de l'UE pour les PME.
- ☐ **Proposer un budget réaliste à la direction**, en tenant compte des contraintes financières de l'organisation.

Validation et engagement de la direction

- ☐ **Préparer une présentation pour la direction**, mettant en avant :
    - Les obligations légales de NIS 2 et les risques de non-conformité (sanctions, responsabilité personnelle des dirigeants).
    - Les bénéfices stratégiques : réduction des risques cyber, renforcement de la résilience, conformité anticipée aux futures réglementations.
    - Le retour sur investissement : diminution des incidents, continuité des activités, renforcement de la confiance des clients et partenaires.
- ☐ **Obtenir l'approbation formelle du plan et du budget**.

Plan de résilience et gestion des risques

- ☐ **Intégrer la gestion des risques cyber dans la stratégie de résilience**.
- ☐ **Pour les Opérateurs d'Importance Vitale (OIV)**, fusionner le **Plan de Sécurité Opérateur (PSO)** et le **Plan de Continuité d'Activité (PCA)** en un **Plan de Résilience Opérateur (PRO)**, à soumettre à l'autorité administrative sous 10 mois.
- ☐ **Prévoir des tests et mises à jour régulières** du plan de résilience au moins tous les 4 ans.

Mise en place d'un suivi et amélioration continue

- ☐ **Planifier des audits préliminaires** pour vérifier l'état de conformité avant les échéances réglementaires.
- ☐ **Réévaluer et ajuster régulièrement** le plan en fonction :

- Des évolutions réglementaires.
- Des nouvelles menaces cyber.
- Des retours d'expérience des audits et incidents passés.

☐ **Utiliser les ressources de l'ANSSI** (Mon Espace NIS 2, guides pratiques) pour adapter les actions en fonction des recommandations officielles.

Résultat attendu

Un plan de conformité détaillé, aligné sur les exigences de **NIS 2**, validé par la direction et soutenu par un budget réaliste, garantissant une mise en œuvre efficace et une résilience accrue face aux cybermenaces.

Étape 5 : Mise en œuvre concrète des mesures techniques et organisationnelles pour la conformité NIS 2 et le renforcement de la résilience opérationnelle

Contexte

Cette phase fondamentale marque la traduction opérationnelle du plan de conformité en actions concrètes. Elle implique le déploiement effectif des mesures techniques, opérationnelles et organisationnelles identifiées lors de l'analyse des écarts et planifiées à l'étape précédente. L'objectif principal est de gérer les risques qui menacent la sécurité des réseaux et systèmes d'information utilisés par l'entité, de prévenir et détecter les incidents, et de minimiser leur impact sur les services fournis et les autres entités. Cette mise en œuvre doit s'inscrire dans une approche multirisque visant à protéger les systèmes d'information et leur environnement physique contre divers types d'incidents. Il est crucial de considérer l'état actuel des connaissances, les normes européennes et internationales pertinentes (comme la série ISO/IEC 27000 pour la sécurité physique et de l'environnement), ainsi que les coûts de mise en œuvre, pour assurer un niveau de sécurité adapté et proportionné aux risques existants. La résilience opérationnelle, c'est-à-dire la capacité à faire face aux incidents de cybersécurité en déployant des plans de gestion des incidents et de continuité d'activité, est un résultat direct de cette étape.

Actions

Mise en place et actualisation des politiques de sécurité

☐ **Élaborer et documenter une politique de gestion des risques cyber** alignée sur **ISO/IEC 27001**.

☐ **Définir une Politique de Sécurité des Systèmes d'Information (PSSI)** couvrant l'ensemble des actifs et processus critiques.

☐ **Mettre en place un cadre de gestion des incidents** avec procédures de **détection, signalement, investigation et réponse aux incidents**.

☐ **Formaliser un Plan de Continuité d'Activité (PCA) et un Plan de Reprise après Sinistre (PRA)**, avec des tests réguliers.

- ☐ **Renforcer la sécurité de la chaîne d'approvisionnement** en évaluant les pratiques de cybersécurité des fournisseurs et en intégrant des **clauses de sécurité contractuelles**.
- ☐ **Établir un cadre de gestion des vulnérabilités** avec procédures de suivi et de correction des failles de sécurité.
- ☐ **Déployer des politiques de cryptographie et de protection des données**, incluant l'usage du **chiffrement** pour les informations sensibles.

Déploiement des solutions techniques de sécurité

- ☐ **Implémenter une authentification forte** (**MFA**) sur les accès aux systèmes critiques.
- ☐ **Déployer un chiffrement robuste** des données **au repos et en transit**.
- ☐ **Installer et configurer des pare-feu et systèmes de détection et prévention d'intrusions (IDPS)**.
- ☐ **Mettre en place une solution de gestion des événements et informations de sécurité (SIEM)** pour une surveillance proactive.
- ☐ **Automatiser la gestion des vulnérabilités et l'application des correctifs**.
- ☐ **Explorer l'usage de l'IA pour la cybersécurité**, notamment pour la détection avancée des menaces.
- ☐ **Sécuriser les communications internes et externes** (voix, vidéo, messagerie) via des canaux chiffrés.
- ☐ **Mettre en œuvre une segmentation réseau stricte** pour limiter la propagation des attaques.

Définition et documentation des processus et procédures

- ☐ **Établir des processus clairs de gestion des incidents** incluant :
    - Identification et classification des incidents.
    - Procédures de réponse et escalade en cas de crise.
    - Plan de communication interne et externe en cas d'incident.
- ☐ **Mettre en place un cadre de gestion des vulnérabilités** avec priorisation selon **l'impact et la criticité**.
- ☐ **Documenter les procédures de sauvegarde et de restauration** des données.
- ☐ **Définir un plan de gestion de crise et des scénarios d'attaque** testés régulièrement.

Renforcement de la sécurité de la chaîne d'approvisionnement

- ☐ **Évaluer la cybersécurité des fournisseurs et prestataires de services critiques**.
- ☐ **Intégrer des exigences de cybersécurité dans les contrats** avec les sous-traitants.
- ☐ **Mettre en place une procédure de due diligence** pour l'évaluation des risques liés aux fournisseurs.
- ☐ **Suivre les recommandations issues des évaluations de risque sectorielles** pour sécuriser la supply chain.

Renforcement de la cyberhygiène et formation à la cybersécurité

- ☐ **Déployer un programme de sensibilisation continue** sur la cybersécurité (phishing, ransomwares, bonnes pratiques).
- ☐ **Former les employés à la gestion des risques et à la réponse aux incidents**.
- ☐ **Appliquer les principes de cyberhygiène** :
    - Mises à jour régulières des systèmes et applications.
    - Gestion rigoureuse des accès utilisateurs (moindre privilège, rotation des mots de passe).
    - Restriction des privilèges administratifs.
    - Sauvegarde régulière des données critiques.

Sécurité des ressources humaines et gestion des accès

- ☐ **Effectuer des vérifications d'antécédents** pour les employés ayant accès à des actifs critiques.
- ☐ **Définir et appliquer des politiques de contrôle d'accès** (Zero Trust, segmentation réseau).
- ☐ **Cartographier et inventorier les actifs critiques** pour assurer une gestion rigoureuse.

Suivi et amélioration continue

- ☐ **Obtenir l'approbation et l'implication de la direction**, qui doit valider et superviser la mise en œuvre.
- ☐ **Évaluer régulièrement la conformité avec des audits internes** et des tests de cybersécurité.
- ☐ **Mettre à jour les politiques et processus en fonction des retours d'expérience et des nouvelles menaces**.
- ☐ **Consulter les guides de l'ANSSI** et suivre les recommandations officielles pour maintenir la conformité.

Résultat attendu

Une organisation résiliente face aux cybermenaces, alignée sur les exigences de **NIS 2**, avec des mesures de sécurité opérationnelles robustes et des processus documentés et testés régulièrement.

Étape 6 : Élaboration et test du plan d'intervention en cas d'incident et du plan de résilience

Contexte

Conformément à la directive NIS 2, il est impératif que les entités essentielles et importantes élaborent et maintiennent des plans robustes pour la gestion et la réponse efficaces aux incidents de cybersécurité, ainsi que pour assurer la continuité de leurs activités et la reprise après sinistre. L'objectif principal de ces plans est de minimiser l'impact des incidents sur la fourniture de leurs services et sur les autres services interconnectés. Ces mesures doivent s'inscrire dans une approche globale de gestion des risques. La directive

insiste sur une préparation à un large éventail de menaces, allant des cyberattaques aux perturbations physiques, adoptant ainsi une approche « tous risques ». Il est fondamental que ces plans soient régulièrement testés et mis à jour afin de garantir leur efficacité face à l'évolution constante des menaces et des vulnérabilités. La capacité à réagir rapidement en cas d'incident de sécurité est cruciale pour en limiter les impacts et pour pouvoir revenir rapidement à une situation normale.

Actions

Élaboration du Plan d'Intervention en Cas d'Incident (PII)

- ☐ **Définir et documenter le plan d'intervention** détaillant :
    - Les rôles et responsabilités des équipes impliquées.
    - Les procédures pour chaque phase d'incident :
        1. **Détection** : identification des signes d'attaque.
        2. **Analyse** : qualification et évaluation de l'impact.
        3. **Confinement** : isolation de l'incident pour éviter la propagation.
        4. **Éradication** : suppression de la menace et assainissement des systèmes.
        5. **Rétablissement** : restauration des services et reprise des activités.
- ☐ **Mettre en place une procédure de notification des incidents** :
    - Informer l'ANSSI sans retard injustifié en cas d'incident significatif.
    - Définir les seuils déclencheurs de notification et les canaux de communication.
    - Intégrer les renseignements sur les menaces (Threat Intelligence) pour affiner la réponse.

Définition du Plan de Résilience des Activités (PRA) et du Plan de Continuité d'Activité (PCA)

- ☐ **Identifier les activités critiques** et les ressources essentielles à leur continuité.
- ☐ **Définir les stratégies de résilience** :
    - Mécanismes de redondance des systèmes critiques.
    - Mise en place de sauvegardes sécurisées et de PRA (Reprise Après Sinistre).
    - Définition des délais de reprise (RTO) et des points de reprise (RPO) pour minimiser les interruptions.
- ☐ **Pour les Opérateurs d'Importance Vitale (OIV)** :
    - Élaborer un Plan de Résilience Opérateur (PRO) conforme aux obligations spécifiques.
    - Intégrer la gestion des crises et les protocoles de prise de décision en cas de perturbation majeure.
- ☐ **Aligner le PRA/PCA avec le Plan de Sécurité Opérateur (PSO)** pour assurer une coordination efficace.

Organisation de simulations et de tests réguliers

- ☐ **Programmer des exercices de simulation pour tester la robustesse des plans** :
    - Tests de réponse aux incidents en condition réelle (exercices « Red Team »).
    - Simulations de cyberattaques et scénarios de crise pour valider les procédures d'escalade.
    - Évaluation des temps de réaction et d'intervention des équipes.
- ☐ **Analyser les résultats et ajuster les plans en conséquence** :
    - Identifier les failles et axes d'amélioration.
    - Modifier les procédures ou renforcer les compétences des équipes si nécessaire.
    - Répéter ces tests périodiquement pour maintenir l'efficacité des plans.

Coordination avec les CSIRT et l'EU-CyCLONe

- ☐ **Se connecter aux équipes de réponse aux incidents de sécurité informatique (CSIRT)** pour bénéficier d'un appui technique et organisationnel en cas de crise.
- ☐ **Intégrer les directives de l'ANSSI et du CERT-FR** pour assurer la conformité nationale.
- ☐ **Anticiper la coopération européenne** via l'EU-CyCLONe pour les incidents à impact transfrontalier.

Intégration avec la gestion des risques et la cyberhygiène

- ☐ **Aligner le plan d'intervention et de résilience avec l'analyse des risques** menée lors des audits.
- ☐ **Mettre en place des pratiques de cyberhygiène rigoureuses** :
    - Mises à jour régulières des systèmes et correctifs de sécurité.
    - Gestion rigoureuse des mots de passe et authentification forte.
    - Renforcement des procédures de sauvegarde et de restauration.

Implication et formation de la direction

- ☐ **S'assurer que la direction est impliquée dans l'approbation et la supervision des plans**.
- ☐ **Organiser des sessions de formation pour les dirigeants sur la gestion de crise cyber**.
- ☐ **Mettre en place un reporting régulier** sur l'état de la résilience et les améliorations apportées.

Résultat attendu

Une organisation préparée à faire face aux cyberattaques, capable de réagir rapidement et efficacement pour limiter l'impact des incidents et assurer la continuité des activités.

Étape 7 : Formation et sensibilisation à la cybersécurité conformément à NIS 2

Contexte

La formation et la sensibilisation des employés à la cybersécurité sont reconnues comme des éléments essentiels pour réduire significativement les risques d'incidents de cybersécurité. La directive NIS 2 met un accent particulier sur la formation à la gestion des risques pour l'ensemble du personnel, y compris les membres des organes de direction, soulignant leur responsabilité directe en matière de sécurité au sein de l'organisation. Cette obligation de formation des dirigeants vise à garantir qu'ils possèdent des connaissances et des compétences suffisantes pour identifier les risques, évaluer les pratiques de gestion des risques de cybersécurité et comprendre leur impact sur les services fournis par l'entité. NIS 2 adopte une approche « tous risques », impliquant une sensibilisation à un large éventail de menaces, allant au-delà des seules cyberattaques. La directive encourage également la promotion active de la cyberhygiène auprès de toutes les structures, y compris les PME. L'objectif est de développer une culture de la gestion des risques au sein de l'organisation.

Actions

Développement et déploiement d'un programme de formation à la cybersécurité

- ☐ **Élaborer un programme de formation adapté aux rôles et responsabilités** de chaque employé :
  - Définir un niveau de sensibilisation différent pour les employés, les managers et la direction.
  - Adapter les contenus en fonction des risques spécifiques liés aux postes (ex. finance, IT, RH).
- ☐ **Intégrer les fondamentaux de la cyberhygiène** :
  - Sécurité des mots de passe (ex. MFA, rotation des mots de passe).
  - Détection des tentatives de phishing et d'ingénierie sociale.
  - Importance des mises à jour logicielles et de la configuration sécurisée des équipements.
  - Procédures de signalement des incidents.
- ☐ **Former les employés aux obligations NIS 2** et aux politiques de sécurité de l'organisation.

Organisation de sessions de sensibilisation régulières

- ☐ **Mettre en place un calendrier annuel de sensibilisation** :
  - Ateliers pratiques, webinaires, e-learning, communications internes.
  - Sessions adaptées au contexte métier de chaque service.
- ☐ **Maintenir l'engagement des employés** en variant les formats :
  - Cas pratiques et scénarios d'attaque simulés.

- Retours d'expérience sur des cyberattaques réelles.
- Utilisation de quiz interactifs et de certifications internes.

☐ **Organiser des tests de sensibilisation** :

- Simulations de phishing pour mesurer la vigilance des employés.
- Exercices de réaction face à un incident cyber (ex. ransomware).
- Analyse des résultats et amélioration continue des formations.

Formation spécifique pour la direction et les décideurs

☐ **Former les dirigeants aux responsabilités juridiques et stratégiques liées à NIS 2** :

- Comprendre l'impact des cyberattaques sur la continuité d'activité et la réputation.
- Intégrer la cybersécurité dans les décisions stratégiques et la gestion des risques.
- Anticiper les sanctions et implications financières en cas de non-conformité.

☐ **Sensibiliser la direction à la gestion de crise cyber** :

- Définition des rôles et processus de prise de décision en cas d'attaque.
- Communication de crise (interne et externe).
- Relation avec les autorités (ANSSI, régulateurs).

Mise en place de bonnes pratiques de cyberhygiène

☐ **Appliquer une politique de gestion des mots de passe robustes** :

- Utilisation de gestionnaires de mots de passe et MFA obligatoire.
- Formation des utilisateurs aux risques liés aux mots de passe faibles.

☐ **Sensibiliser les employés aux risques numériques et aux bonnes pratiques** :

- Affichage et diffusion de guides pratiques sur la cybersécurité.
- Intégration de modules de sensibilisation lors de l'onboarding des nouveaux arrivants.

Évaluation et amélioration continue des formations

☐ **Mesurer l'efficacité des formations** à travers :

- Des tests de connaissance avant/après les sessions.
- Le suivi des comportements des employés (ex. taux de clic sur des emails de phishing simulés).

☐ **Adapter régulièrement les contenus** en fonction des nouvelles menaces et des résultats des audits internes.

☐ **Suivre les recommandations de l'ANSSI** et utiliser les ressources mises à disposition pour renforcer les modules de formation.

Résultat attendu

Une organisation où chaque employé et dirigeant est conscient des risques cyber, applique des bonnes pratiques et contribue activement à la sécurisation des systèmes conformément à **NIS 2**.

Étape 8 : Mise en place des processus de détection et de notification des incidents conformément à NIS 2

Contexte

La directive NIS 2 impose aux entités essentielles (EE) et aux entités importantes (EI) l'obligation de mettre en place des mécanismes robustes pour détecter les incidents de sécurité affectant leurs réseaux et systèmes d'information. Une fois un incident significatif détecté, elles doivent le notifier sans retard injustifié aux autorités compétentes, qui est l'ANSSI en France. La notification d'un incident important doit être effectuée selon un mécanisme échelonné, avec une alerte précoce dans les 24 heures suivant la prise de connaissance de l'incident [notre conversation historique, 41, 56, 92, 144]. Cette obligation de notification vise à permettre une réaction rapide pour limiter les impacts et à favoriser le partage d'informations au niveau national et européen. Il est crucial de noter que la simple notification d'un incident n'expose pas l'entité notificatrice à une responsabilité accrue.

Actions

Mise en place des outils et processus de surveillance des incidents

- ☐ **Déployer un système de détection et de gestion des incidents** :
  - Installer des systèmes de détection d'intrusion (IDS/IPS) pour identifier les activités malveillantes.
  - Mettre en place une solution SIEM (Security Information and Event Management) pour une surveillance et une corrélation des événements en temps réel.
  - Intégrer des outils de threat intelligence pour anticiper les menaces émergentes et hiérarchiser les alertes critiques.
  - Automatiser l'analyse et l'investigation des incidents via des outils de SOAR (Security Orchestration, Automation and Response).
- ☐ **Établir une procédure d'investigation des incidents** :
  - Définir les responsabilités de chaque équipe dans la gestion d'un incident.
  - Assurer une traçabilité complète des événements pour faciliter les audits et la réponse aux incidents.

Définition des critères de classification des incidents

- ☐ **Définir une grille de criticité des incidents** basée sur :
  - L'impact sur les opérations (interruption de service, pertes financières, atteinte aux données).
  - Le caractère systémique ou récurrent de l'incident.
  - La présence d'un impact transfrontalier ou d'un acte malveillant suspecté.

- ☐ **Aligner la classification des incidents avec les critères définis par la Commission européenne et l'ANSSI**.
- ☐ **Intégrer une approche proactive** en analysant les incidents récurrents pouvant révéler des faiblesses structurelles.

Mise en place d'un processus de notification des incidents à l'ANSSI

- ☐ **Définir une procédure de notification en plusieurs étapes** :
  - **Alerte précoce** (**early warning**) dans les **24 heures** après identification de l'incident, mentionnant :
    - La suspicion d'un acte malveillant ou illicite.
    - L'éventuel impact transfrontalier.
  - **Notification complète sous 72 heures (24h pour les prestataires de services de confiance), comprenant :**
    - Une mise à jour des informations de l'alerte précoce.
    - Une évaluation de l'impact et des indicateurs de compromission (IOCs).
  - **Rapport intermédiaire si nécessaire, à la demande du CSIRT.**
  - **Rapport final sous un mois, une fois l'incident totalement traité.**
- ☐ **Mettre en place un canal de communication sécurisé pour les échanges avec l'ANSSI**.
- ☐ **Documenter chaque notification d'incident** pour assurer la traçabilité des actions et justifier la conformité en cas de contrôle.

Formation et sensibilisation des employés au signalement des incidents

- ☐ **Élaborer des procédures claires de signalement** pour permettre aux employés de déclarer rapidement un incident.
- ☐ **Communiquer largement ces procédures via** :
  - Des guides internes et supports pédagogiques.
  - Des sessions de formation intégrant des mises en situation réelles.
  - Des tests de détection pour évaluer la réactivité des équipes face aux incidents.
- ☐ **Intégrer la gestion des incidents dans les exercices de sensibilisation et de simulation** (ex. cyberattaques fictives).

Communication avec les destinataires des services affectés

- ☐ **Informer rapidement les clients et partenaires** lorsqu'un incident impacte leurs services.
- ☐ **Fournir des recommandations pour minimiser les risques secondaires** :
  - Mesures de précaution à adopter.
  - Correctifs ou solutions temporaires mises en place.

- ☐ **Mettre en place un plan de gestion de crise communicationnelle** en cas d'incident critique.

Intégration avec les exigences du RGPD et des autres régulations

- ☐ **S'assurer que la notification des incidents respecte les obligations du RGPD en cas de fuite de données personnelles**.
- ☐ **Garantir la confidentialité des informations transmises à l'ANSSI**.
- ☐ **Aligner les processus de déclaration avec les autres régulations sectorielles applicables** (ex. DORA pour le secteur financier).

Résultat attendu

Une organisation équipée d'outils performants de détection des incidents, capable de réagir rapidement et de notifier efficacement les incidents critiques aux autorités, conformément aux exigences de **NIS 2**.

Étape 9 : Audits internes et amélioration continue conformément à NIS 2

Contexte

La conformité à la directive NIS 2 n'est pas un état statique, mais un processus continu qui nécessite une amélioration constante pour maintenir un niveau de cybersécurité adéquat face à l'évolution des menaces et des exigences réglementaires [notre conversation historique]. Des audits internes réguliers sont essentiels pour vérifier l'efficacité des mesures de gestion des risques de cybersécurité mises en place et pour identifier les points faibles et les domaines nécessitant des améliorations. Ces audits contribuent à assurer la résilience opérationnelle des entités essentielles (EE) et importantes (EI).

Actions

Planification et réalisation d'audits internes réguliers

- ☐ **Établir un programme d'audit périodique** en fonction de :
  - L'évaluation des risques et la criticité des activités.
  - Les obligations de conformité à NIS 2 et aux référentiels de sécurité (ex. ISO 27001).
- ☐ **Définir le périmètre des audits** couvrant :
  - Politiques et procédures de sécurité des SI.
  - Gestion des incidents et plans de continuité d'activité.
  - Sécurité de la chaîne d'approvisionnement et contrôle des sous-traitants.
  - Sécurité dans le développement et la maintenance des SI.
  - Pratiques de cyberhygiène et formation à la cybersécurité.

- Sécurité des ressources humaines, contrôle d'accès et authentification multifactorielle.

☐ **Effectuer des tests complémentaires pour valider la posture de sécurité** :

- Tests de pénétration (pentests) pour évaluer la robustesse des systèmes.
- Audits de configuration pour identifier les erreurs et failles de paramétrage.
- Simulations d'incidents et exercices de crise pour tester la résilience.

Exploitation des résultats des audits et mise en œuvre des actions correctives

☐ **Analyser et documenter les faiblesses identifiées** dans un rapport d'audit structuré.

☐ **Élaborer un plan d'action correctif** avec :

- Priorisation des non-conformités critiques et des vulnérabilités exploitées.
- Identification des responsables de mise en œuvre pour chaque action.
- Définition d'échéances claires et d'un suivi des actions.

☐ **Mettre en place un tableau de bord de suivi** des actions correctives et de leur avancement.

Mise à jour des politiques et procédures en fonction des nouvelles menaces

☐ **Effectuer une veille continue sur les évolutions des menaces cyber et des obligations réglementaires** :

- Exploiter les rapports de Threat Intelligence (veille sur les cyberattaques ciblant l'organisation ou son secteur).
- Suivre les recommandations des autorités compétentes (ex. ANSSI, ENISA, CSIRT).

☐ **Réviser régulièrement les politiques de sécurité et les procédures opérationnelles** pour :

- Intégrer les nouveaux risques identifiés lors des audits et incidents récents.
- Adapter les mesures de protection aux nouvelles attaques et vulnérabilités.
- Tenir compte des évaluations de la sécurité des chaînes d'approvisionnement et des sous-traitants critiques.

☐ **Imposer une mise à jour formelle des analyses de risques** au moins tous les **4 ans pour les OIV** et en fonction de l'évolution du contexte pour les autres entités.

Évaluation de l'efficacité des mesures de gestion des risques

☐ **Mettre en place des indicateurs de performance de la cybersécurité** :

- Taux de correction des vulnérabilités dans les délais définis.
- Temps moyen de détection et de réponse aux incidents.
- Nombre d'incidents de sécurité impactant les opérations.

☐ **Réaliser des exercices pratiques et simulations de cyberattaques** :

- Organiser des exercices en équipe rouge (Red Team) et en équipe bleue (Blue Team).
- Participer aux exercices de cybersécurité européens organisés par l'ENISA.

Implication de la direction dans l'amélioration continue

- ☐ **Présenter régulièrement les résultats des audits à la direction** pour :
  - Obtenir une validation et un engagement formel sur les mesures à mettre en œuvre.
  - Assurer l'allocation des ressources nécessaires pour améliorer la sécurité.
- ☐ **Intégrer la cybersécurité dans la stratégie de gestion des risques de l'entreprise**.
- ☐ **Encourager une culture de cybersécurité proactive** à travers des programmes de formation et de sensibilisation basés sur les retours d'audits.

Résultat attendu

Une organisation en conformité continue avec **NIS 2**, capable d'identifier, d'évaluer et de corriger efficacement ses failles de cybersécurité pour une résilience optimale.

Étape 10 : Préparation aux contrôles externes et aux évolutions futures

Contexte

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité compétente en France pour contrôler la conformité à la directive NIS 2. Il est donc crucial de se préparer activement à d'éventuels contrôles externes, tels que des inspections sur site et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés. De plus, le paysage technologique et les menaces cyber évoluent constamment, nécessitant une adaptation continue des mesures de sécurité pour maintenir un niveau de protection efficace.

Actions

Maintien d'une documentation complète et accessible pour les contrôles

- ☐ **Organiser et mettre à jour un référentiel documentaire centralisé** contenant :
  - Les politiques et procédures de cybersécurité mises en place.
  - Les résultats des audits de sécurité internes et externes.
  - Les plans de gestion des risques, de réponse aux incidents et de continuité d'activité (PCA/PRA).
  - Les registres des formations à la cybersécurité suivies par les employés et la direction.

- ☐ **Veiller à l'accessibilité des documents clés** pour démontrer la conformité en cas d'inspection de l'ANSSI.
- ☐ **S'assurer que la documentation répond aux exigences de l'article 21 de la directive NIS 2** et qu'elle est prête à être communiquée lors des contrôles.

Suivi des directives et recommandations de l'ANSSI

- ☐ **Mettre en place une veille réglementaire sur l'application de NIS 2 en France** via :
  - Le portail Mon Espace NIS 2 de l'ANSSI et ses mises à jour régulières.
  - Les publications officielles et guides de conformité de l'ANSSI et de l'ENISA.
  - La participation à des webinaires et conférences sur NIS 2 pour anticiper les attentes des contrôleurs.
- ☐ **Intégrer les nouvelles recommandations de l'ANSSI dans les politiques de cybersécurité internes**.

Anticipation des évolutions technologiques et réglementaires

- ☐ **Prendre en compte l'évolution des technologies et intégrer une clause d'adaptabilité** :
  - Suivre les recommandations de la Commission supérieure du numérique et des postes (CSNP) sur l'intelligence artificielle en cybersécurité.
  - Explorer l'usage de technologies innovantes (IA, analyse comportementale, automatisation) pour améliorer la détection et la prévention des cyberattaques.
- ☐ **Assurer une veille sur les évolutions réglementaires et législatives** :
  - Suivre les mises à jour de la transposition de NIS 2 en droit français.
  - Anticiper les interactions avec d'autres réglementations telles que DORA (secteur financier) et les exigences spécifiques aux opérateurs d'importance vitale (OIV).
  - Préparer l'organisation à des exigences de cybersécurité renforcées en lien avec les nouvelles menaces.

Préparation proactive aux contrôles externes et audits ANSSI

- ☐ **Effectuer des audits internes préliminaires réguliers** pour identifier et corriger les écarts avant un contrôle officiel :
  - Simuler un audit ANSSI avec des équipes internes ou externes spécialisées.
  - Vérifier la bonne application des politiques de cybersécurité et la traçabilité des actions.
- ☐ **Mettre en place un plan de réponse aux contrôles** avec :
  - Un responsable de conformité NIS 2 chargé de coordonner les réponses aux demandes des contrôleurs.
  - Une procédure interne pour réagir aux demandes d'information de l'ANSSI.
  - Un plan d'action correctif en cas d'identification de non-conformités.

Résultat attendu

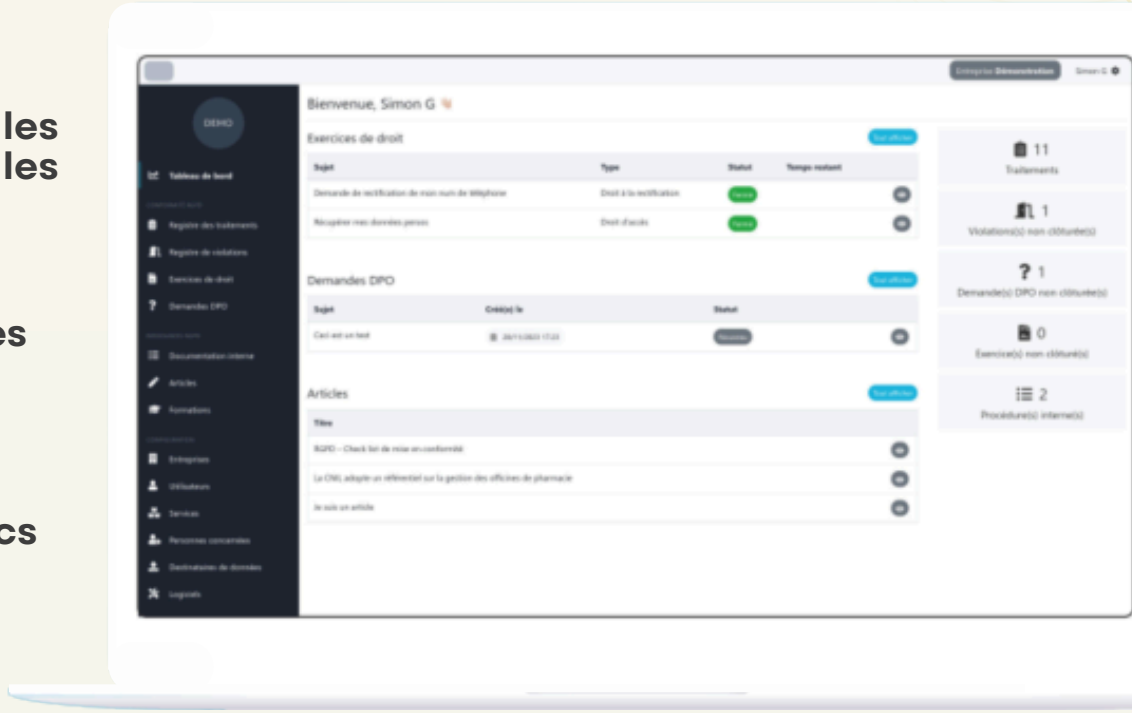
Une organisation prête à faire face aux **contrôles externes**, capable de démontrer sa conformité **de manière fluide et structurée**, tout en anticipant les évolutions réglementaires et technologiques liées à **NIS 2**.

PRODPO - LE LOGICIEL IDÉAL DU DPO

Simplifier la gestion de conformité RGPD dans votre organisation

ProDPO est une solution logicielle conçue pour les Délégués à la Protection des Données (DPO) et les professionnels du RGPD.

- **Interface intuitive et fonctionnalités avancées**
- **Registre de traitement personnalisable**
- **Gestion intégrée des exercices des droits**
- **Gestion des violations et AIPD en quelques clics**

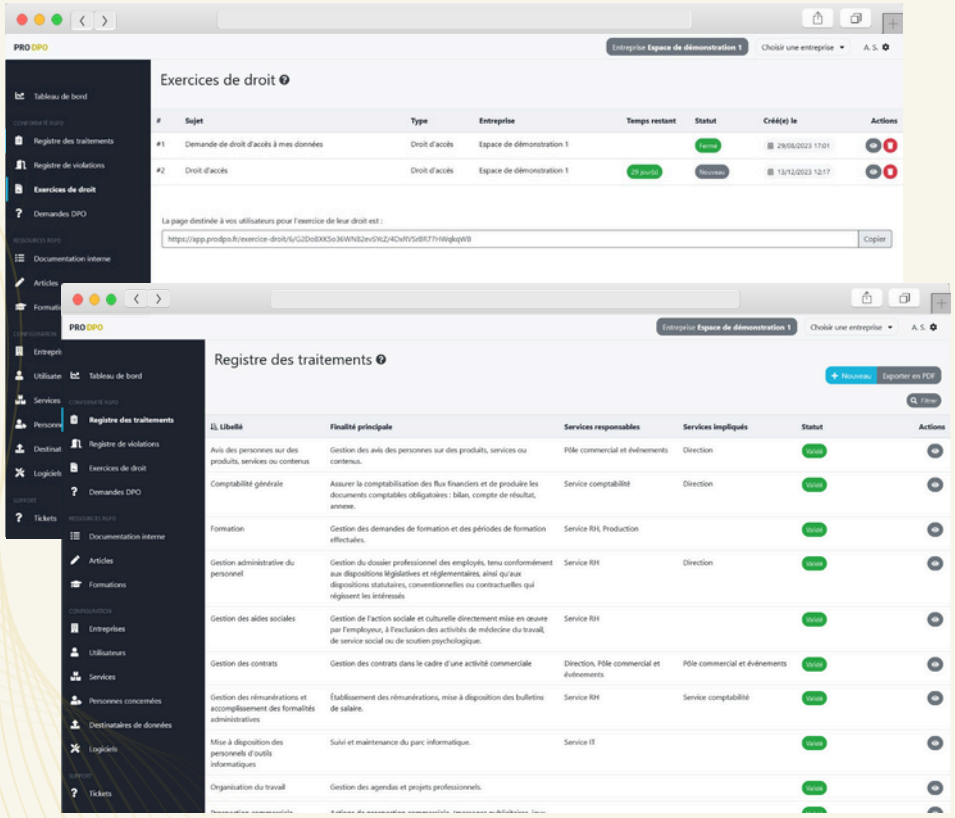


Vous êtes DPO au sein de votre entreprise ou DPO externe de plusieurs organisations, ce logiciel a été pensé pour vous.

PRODPO

FONCTIONNALITÉS INNOVANTES

POUR UNE GESTION RGPD EFFICACE



Registre de traitement

ProDPO personnalise et préconfigure un registre des activités de traitement pour vous. Le logiciel intègre une base de traitements standards adaptée à votre secteur ou à ceux de vos clients.

Tableau de bord intuitif

ProDPO vous propose une vue d'ensemble conçue pour offrir une compréhension instantanée, ce tableau de bord transforme les données complexes en insights actionnables.

Gestion des exercices des droits

ProDPO révolutionne la gestion des exercices de droits avec un formulaire personnalisé pour votre entreprise ou celle de vos clients. Cette centralisation permet une gestion efficace et transparente des demandes des personnes concernées.

ProDPO n'est pas seulement un logiciel, c'est un partenaire stratégique dans la protection et la gestion des données personnelles.

FONCTIONNALITÉS INNOVANTES

POUR UNE GESTION RGPD EFFICACE

Gestion des violations de données

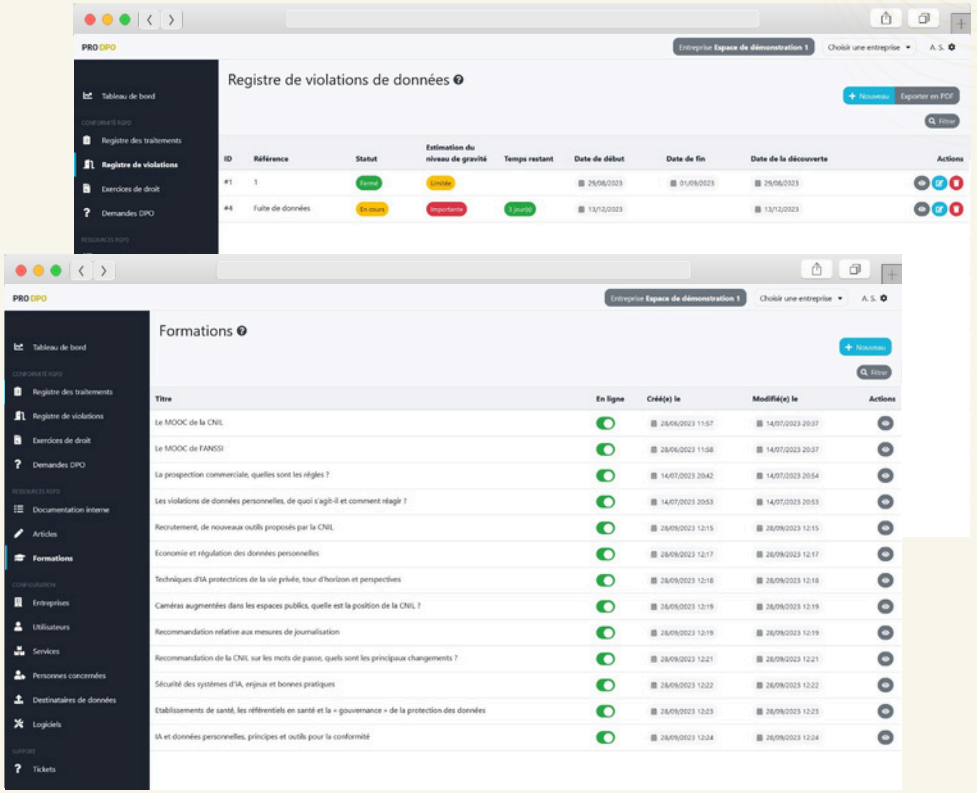
Face à une violation de données, la réactivité est cruciale. ProDPO vous permet de gérer efficacement ces situations critiques en vous aidant à documenter la violation et à préparer vos déclarations à la CNIL.

Documentation RGPD

ProDPO sera votre bibliothèque centralisée de procédures et de documentations RGPD. Organisez et stockez tous vos documents, et facilitez la signature électronique par vos collaborateurs.

Formation RGPD et Cybersécurité

Grâce à des contenus gratuits et régulièrement mis à jour, ProDPO va au-delà de la simple conformité en intégrant une plateforme de formation sur le RGPD et la cybersécurité.



ProDPO n'est pas seulement un logiciel, c'est un partenaire stratégique dans la protection et la gestion des données personnelles.

NOS OFFRES

Abonnements flexibles

FORMULE DPO INTERNE

Parfaite pour les DPO opérant en interne, cette formule offre un accès illimité aux utilisateurs et inclut toutes les fonctionnalités essentielles pour une gestion complète de la conformité RGPD.

À partir de 28 € / mois

FORMULE DPO EXTERNE OU MUTUALISÉ

Cette formule transforme la gestion de la conformité RGPD grâce à une plateforme unique permettant de gérer tous vos comptes clients.

Elle optimise le passage d'un client à l'autre pour un gain de temps et d'efficacité. Elle permet aussi d'enrichir la base standard avec des traitements spécifiques à chacun des secteurs de vos clients, offrant une gestion de la conformité sur mesure.

ProDPO s'adapte et évolue selon vos besoins, quelle que soit la taille de votre entreprise.

À partir de 28 € / mois - Prix dégressif

ProDPO est plus qu'un logiciel de conformité RGPD ; c'est un écosystème complet qui équipe les DPO et les entreprises avec les outils nécessaires pour naviguer avec confiance dans le paysage complexe de la protection des données.

En choisissant ProDPO, vous optez pour une solution qui allie innovation, sécurité, et expertise pour transformer la manière dont votre organisation gère la conformité RGPD.

Rejoignez les organisations qui font confiance à ProDPO pour leur conformité RGPD. Contactez-nous dès aujourd'hui pour une démonstration personnalisée et découvrez comment ProDPO peut transformer la gestion de vos données.

WWW.PRODPO.FR