SYNTHÈSE DU GUIDE DE L'ENISA SUR LES MESURES DE GESTION DES RISQUES EN CYBERSÉCURITÉ (NIS2)

Résumé à destination des **décideurs, responsables conformité, RSSI et parties prenantes non techniques.**

OBJECTIF DU DOCUMENT

Ce document synthétise les recommandations de l'ENISA relatives à la mise en œuvre des mesures de gestion des risques en cybersécurité, prévues par le règlement (UE) 2024/2690 dans le cadre de la directive NIS2. Il a pour but d'accompagner les entités dans l'implémentation de bonnes pratiques de cybersécurité adaptées à leur contexte.

SYNTHÈSE DU GUIDE DE L'ENISA

SUR LES MESURES DE GESTION DES RISQUES EN CYBERSÉCURITÉ (NIS2)

PUBLIC CONCERNÉ

Ce guide est destiné aux entités essentielles ou importantes soumis à la directive NIS2. Ce guide peut également être utilisé par des entités publiques ou privés pour améliorer leur maturité cyber.

SOMMAIRE

RÉSUMÉ DES 13 DOMAINES :

RÉSUMÉ DES 13 DOMAINES

1 Politique de sécurité des systèmes d'information

OBJECTIF

Définir une stratégie claire de la cybersécurité, validée par la direction avec des objectifs, des rôles et une diffusion appropriée.

POINTS CLÉS

- Élaborer un document stratégique approuvé par la direction.
- Y intégrer les objectifs de sécurité, les rôles et responsabilités, les ressources allouées.
- S'assurer que tous les employés et partenaires concernés le connaissent.
- Revoir cette politique chaque année ou après un incident majeur.

PREUVES

- Politique de sécurité des systèmes d'information (PSSI), signée par la direction.
- Preuves de communication interne (emails, réunions).
- Accusés de réception signés par les employés et partenaires.
- Liste des politiques spécifiques mentionnées.
- Revue annuelle de la politique.

2 Politique de gestion des risques

Mettre en place une démarche de gestion des risques structurée (analyse, traitement, acceptation), révisée régulièrement.

OBJECTIF

Identifier, évaluer et traiter les risques pesant sur les systèmes d'information.

POINTS CLÉS

- Définir une méthodologie pour analyser les risques (internes, externes, liés aux tiers).
- Créer un plan de traitement des risques (réduction, transfert, acceptation).
- Réaliser une évaluation annuelle ou lors de changements significatifs.
- Associer cette politique aux enjeux métiers et aux analyses d'impact.

PREUVES

- Méthodologie documentée de gestion des risques.
- Plan de traitement des risques.
- Liste des risques identifiés et leur criticité.
- Preuves de mise à jour annuelle.

3 | Gestion des incidents

Prévoir des procédures de détection, réponse, communication et analyse post-incident. Réaliser des tests réguliers.

OBJECTIF

Être capable de détecter, répondre et se remettre rapidement d'un incident cyber.

POINTS CLÉS

- Définir un processus clair pour détecter, contenir, analyser et résoudre les incidents.
- Établir des rôles précis et des plans de communication (interne et externe).
- Effectuer des exercices de gestion de crise pour se préparer aux incident et en lien avec les plans de continuité et de reprise d'activité.

PREUVES

- Politique de gestion des incidents.
- Plans de communication d'incident.
- Procédures de classification et d'escalade des incidents.
- Résultats et retour d'expérience des exercices effectuées.
- Registre des incidents passés.

4 | Continuité d'activité et gestion de crise

Assurer une continuité de service même en cas d'incident grave, via des PCA/PRA testés et documentés.

OBJECTIF

Garantir la résilience des activités même en cas de cyberattaque.

POINTS CLÉS

- Élaborer un plan de reprise (PRA) et un plan de continuité d'activité (PCA).
- Prévoir des solutions de sauvegarde, de redondance et des alternatives en cas de panne.
- Organiser régulièrement des tests de ces dispositifs.

PREUVES

- Plans PCA/PRA documentés.
- Résultats de tests de continuité.
- Cartographie des systèmes critiques.
- Liste des ressources de secours et redondances.

5 | Sécurité de la chaîne d'approvisionnement

Suivre les fournisseurs critiques, imposer des clauses de sécurité, et vérifier leur conformité en continu.

OBJECTIF

Réduire les risques liés aux fournisseurs, sous-traitants et partenaires.

POINTS CLÉS

- Tenir un registre des fournisseurs critiques.
- Exiger des engagements de sécurité dans les contrats (PAS : Plan Assurance Sécurité).
- Suivre et auditer les fournisseurs régulièrement.
- Prendre en compte les dépendances logicielles (open source inclus).

PREUVES

- Contrats fournisseurs avec clauses de sécurité.
- Liste des fournisseurs critiques.
- Preuves d'audits ou d'évaluations de conformité des prestataires.
- Journal des incidents liés aux tiers.

6 | Sécurité dans l'acquisition, le développement et la maintenance

Intégrer la sécurité dès la conception et tout au long du cycle de vie des systèmes, y compris patching et segmentation réseau.

OBJECTIF

Intégrer la sécurité dès la conception des systèmes et services numériques.

POINTS CLÉS

- Intégrer la cybersécurité dans les appels d'offre, contrats, etc.
- Mettre en œuvre un cycle de développement sécurisé.
- Gérer les configurations, changements, mises à jour et correctifs.
- Protection contre les logiciels malveillants et gestion des vulnérabilités connues.

PREUVES

- Politique d'acquisition sécurisée.
- Procédures de gestion des changements et configurations.
- Résultats de tests de sécurité (pentests, scans).
- Registre des mises à jour et correctifs appliqués.

7 | Évaluation de l'efficacité des mesures

Mesurer régulièrement la performance des dispositifs de sécurité en place, et ajuster les plans en conséquence.

OBJECTIF

Vérifier régulièrement que les actions de sécurité sont efficaces.

POINTS CLÉS

- Mettre en place d'indicateurs et de revues périodiques.
- Effectuer des audits, des tests, ou utiliser outils de contrôle.
- Corriger les écarts constatés et formaliser leur traitement.

PREUVES

- Rapports d'audit internes ou externes.
- Indicateurs de performance (KPI) sécurité.
- Procédures de revue et d'amélioration continue.
- Plans d'action de déploiement des correctifs documentés.

8 | Bonnes pratiques d'hygiène numérique et formation

Former le personnel, promouvoir les bons réflexes de sécurité (phishing, mots de passe, etc.).

OBJECTIF

Sensibiliser les employés et renforcer la connaissance des risques cyber au sein de l'entité.

POINTS CLÉS

- Former régulièrement tous les collaborateurs, selon leur niveau de responsabilité et leur fonction.
- Mettre en place des rappels réguliers sur les bonnes pratiques (mots de passe, phishing, etc.).
- Intégrer la cybersécurité dans les processus RH (e.g. mouvement de personnel).

PREUVES

- Programmes de formation et supports utilisés lors des sessions.
- Feuilles de présence ou attestations de participation.
- Campagnes de sensibilisation (affiches, emails, newsletters).

9 | Cryptographie

Utiliser le chiffrement pour protéger les données sensibles. Gérer les clés et algorithmes de manière rigoureuse.

OBJECTIF

Protéger les données sensibles par des méthodes de chiffrement adaptées.

POINTS CLÉS

- Utiliser des solutions de chiffrement appropriées pour les données sensibles.
- Gérer les clés de manière sécurisée.
- Appliquer des normes reconnues, éviter les algorithmes obsolètes.

PREUVES

- Politique de chiffrement documentée.
- Liste des outils ou algorithmes utilisés.
- Journal de gestion des clés.
- Vérifications de conformité aux normes (ex : ISO, eIDAS).

10 | Sécurité des ressources humaines

Encadrer les pratiques RH liées à la sécurité : vérification d'antécédents, gestion des départs, confidentialité.

OBJECTIF

Intégrer la cybersécurité dans la gestion des collaborateurs.

POINTS CLÉS

- Vérifier les antécédents pour les postes sensibles.
- Prévoir des procédures claires pour l'arrivée et le départ des employés.
- Sensibiliser au respect des politiques internes et prévoir un cadre disciplinaire (e.g. charte informatique).

PREUVES

- Procédures de mouvement de personnel (arrivée, mutation et départ).
- Contrats avec clauses de confidentialité.
- Historique des actions disciplinaires (si existantes).
- Contrôles d'antécédents (si requis).

11 | Contrôle des accès

Limiter les accès selon les besoins, activer l'authentification forte, gérer les comptes à privilèges.

OBJECTIF

S'assurer que chaque utilisateur accède uniquement aux ressources nécessaires.

POINTS CLÉS

- Mettre en place une politique de gestion des accès basée sur le principe du "moindre privilège".
- Gérer les comptes privilégiés avec des protections renforcées (e.g. MFA, supervision).
- Réaliser des revues régulières des droits d'accès.

PREUVES

- Politique de gestion des accès.
- Registre des droits d'accès et des comptes.
- Résultats de revues d'accès périodiques.
- Mise en œuvre de l'authentification forte (MFA).

12 | Gestion des actifs

Inventorier et classifier les actifs IT, contrôler l'usage des supports amovibles et les restitutions d'équipement.

OBJECTIF

Maintenir une vue claire et à jour des équipements et données critiques.

POINTS CLÉS

- Tenir un inventaire des actifs (matériels, logiciels, données).
- Définir leur niveau de criticité.
- Gérer les supports amovibles.
- Gérer la restitution ou la destruction des équipements.

PREUVES

- Inventaire des actifs (matériel, logiciel, données).
- Politique sur l'utilisation des supports amovibles.
- Procédures de restitution ou suppression des équipements.

13 | Sécurité physique et environnementale

Sécuriser l'accès aux locaux, prévenir les incidents physiques (incendies, coupures, intrusions).

OBJECTIF

Protéger les locaux, équipements et installations contre les accès non autorisés ou les incidents physiques.

POINTS CLÉS

- Contrôler l'accès aux bâtiments (badges, vidéosurveillance, registre).
- Prévoir des dispositifs contre les incendies, inondations ou coupures d'alimentation.
- Sécuriser les zones critiques (salles serveurs, équipements réseaux).

PREUVES

- Schémas ou plans d'accès aux locaux.
- Dispositifs physiques installés (badge, caméras, alarmes).
- Rapports de tests ou de simulation d'incident (incendie, coupure électrique).

FRANCE CYBER MARITIME

Le Grand Large,
Quai de la douane, 2ème éperon,
29200 BREST

NOUS CONTACTER

02 57 52 09 87
contact@france-cyber-maritime.eu

www.france-cyber-maritime.eu

AVEC LE SOUTIEN DE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

Brest Métropole

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE, DE LA BIODIVERSITÉ, DE LA FORÊT, DE LA MER ET DE LA PÊCHE

Région Bretagne

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la mer