NIS2, sensibilisation cybersécurité et devoir de diligence

Pourquoi le « tick the box » ne suffit plus

Comment piloter une stratégie de sensibilisation conforme, mesurable et défendable face à NIS2

conscio Technologies

NIS2, sensibilisation cybersécurité et devoir de diligence

Pourquoi le « tick the box » ne suffit plus

Comment piloter une stratégie de sensibilisation conforme, mesurable et défendable face à NIS2

Un livre blanc édité par

conscio Technologies

Sommaire

Avant-propos

La directive NIS2 redéfinit en profondeur les attentes de l'Union européenne en matière de cybersécurité. Au-delà des nouvelles obligations de gouvernance, de gestion des risques et de notification d'incidents, elle introduit **une exigence plus discrète mais structurante** : la responsabilisation des dirigeants et la nécessité de pouvoir démontrer, à tout moment, que les mesures prises sont « appropriées et proportionnées ».

Pour la sensibilisation des collaborateurs, cette évolution change la donne. Il ne s'agit plus seulement de diffuser des contenus pour pouvoir cocher la case « formation des utilisateurs » : il faut désormais être capable de démontrer que l'on a fait ce qu'un acteur raisonnable et prudent ferait dans le même contexte. Autrement dit, qu'on a fait preuve d'un véritable devoir de diligence.

Ce livre blanc s'adresse aux RSSI, DSI et responsables conformité qui souhaitent comprendre concrètement ce que NIS2 implique pour leur stratégie de sensibilisation, et identifier les leviers à activer pour passer d'une **logique de couverture documentaire à une logique de résultats mesurables**.

Il est issu de nos échanges avec plus d'une centaine de clients en 2025-2026, et nourri par les résultats d'une étude d'impact menée auprès de plus de 7 000 répondants sur l'année 2025.

À retenir en une phrase

NIS2 n'impose pas de contenus spécifiques de sensibilisation, mais introduit une exigence de résultat : être capable de démontrer que la démarche est structurée, mesurée et continue.“

PARTIE 1

NIS2 et sensibilisation : ce qui change vraiment

› Pas de contenus spécifiquement « NIS2 »

Une idée reçue mérite d'être déconstruite d'emblée : NIS2 ne définit ni programme, ni thématiques, ni format imposé pour la sensibilisation. Sur ce point, la directive est exactement dans la même logique que le RGPD ou la famille de normes ISO 2700x. Elle se borne à stipuler que **la sensibilisation des utilisateurs est obligatoire**.

Les thématiques de fond restent celles que tout RSSI connaît bien : protection de l'information, hygiène des mots de passe, phishing, ingénierie sociale, codes malveillants, mobilité, postures BYOD. À cela s'ajoutent au fil de l'eau les sujets plus contemporains : clickfix, signalement des événements, shadow IT, quishing, deepfakes, abus de l'IA générative.

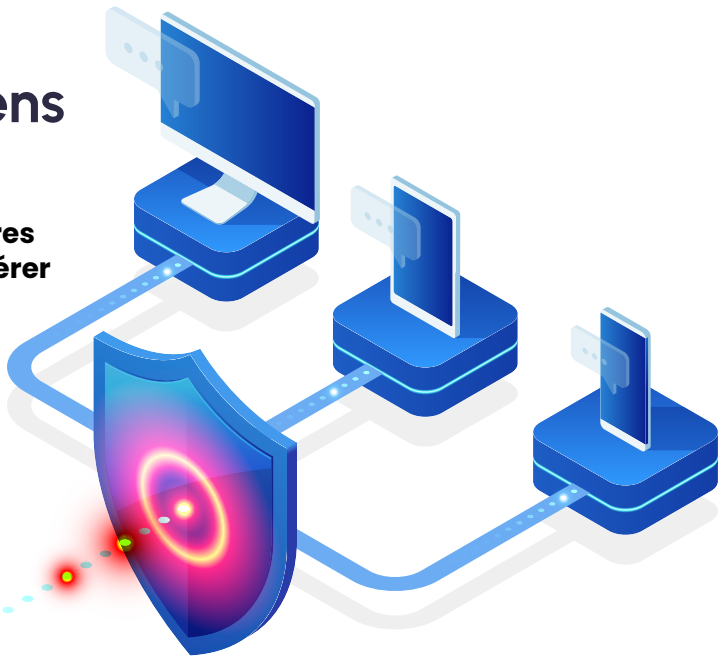
Conséquence pratique

Les contenus que vous diffusez déjà à vos collaborateurs sont, en règle générale, conformes à NIS2. Inutile de tout reconstruire au prétexte de la directive. Le sujet n'est pas le « quoi », c'est le « comment » et surtout le « avec quels résultats ».

› Ce qui change : une obligation de moyens renforcée

L'article 21 de la directive exige des mesures « appropriées et proportionnées » pour gérer les risques de cybersécurité. Le terme « appropriées » est central : il ne renvoie pas à une liste prescriptive, mais à un standard implicite — celui de ce que ferait, dans le même contexte, une entité comparable, raisonnablement prudente.

C'est précisément ce déplacement, du contenu vers la démarche, que ce livre blanc se propose d'éclairer.



PARTIE 2

Le devoir de diligence, nouveau standard juridique

Une logique simple, des conséquences profondes

Le devoir de diligence repose sur un principe élémentaire : **une entité ne peut pas se contenter de faire le minimum**, simplement pour cocher une case. Elle doit faire ce qu'un acteur raisonnable et prudent ferait dans la même situation, à la lumière des risques connus et des pratiques de son secteur.

La question que posera un juge ou un auditeur

« Avez-vous fait tout ce qu'on pouvait raisonnablement attendre de vous pour que vos collaborateurs adoptent les bons comportements ? »

Le précédent RGPD : un avertissement à entendre

L'histoire récente du contentieux RGPD est éclairante. La CNIL et ses homologues européens ont déjà sanctionné des organisations non pas parce qu'elles n'avaient rien fait, mais parce que ce qu'elles avaient fait était jugé **insuffisant au regard des risques encourus et des pratiques courantes du secteur**.
Tout indique que NIS2 suivra la même logique. Un dispositif de sensibilisation purement déclaratif, sans démarche d'amélioration continue ni mesure de résultats, sera difficile à défendre en cas d'incident grave (fuite de données, indisponibilité prolongée, compromission d'une chaîne d'approvisionnement).

Trois implications concrètes pour le RSSI

- ✔ **Documenter la démarche, pas seulement les actions.** Les choix de scénarios, de cibles, de fréquence et de canaux doivent être tracés et justifiés.
- ✔ **Se référer à des standards externes.** Benchmarks sectoriels, recommandations ENISA, guides ANSSI : autant de jalons utiles pour étalonner le « raisonnable ».
- ✔ **Mesurer et corriger.** Une sensibilisation sans indicateurs d'efficacité et sans boucle d'amélioration sera systématiquement attaquable.

PARTIE 3

La fin de la sensibilisation « *tick the box* »

Pendant longtemps, la sensibilisation cybersécurité a été traitée comme une obligation administrative : diffuser un module d'e-learning, faire signer une charte, archiver les preuves de participation. Cette approche a vécu. NIS2, en consacrant le devoir de diligence, achève de la disqualifier.

Le benchmark comme étalon de diligence

La question pertinente n'est plus « avons-nous formé nos collaborateurs ? » mais « qu'est-ce qu'une organisation comparable fait, et avec quels résultats ? ». **Le benchmark sectoriel devient ainsi le nouveau référentiel implicite contre lequel les pratiques seront jugées.**

C'est dans cet esprit que Conscio Technologies conduit chaque année une étude d'impact à froid auprès des collaborateurs de ses clients. En 2025, ce sont plus de **7 000 répondants** dont les retours ont été collectés et analysés. Les enseignements de cette étude permettent à chaque client de situer ses propres résultats par rapport à un panel global et d'identifier ses marges de progression.

Identifier les freins à la participation

L'un des apports majeurs de cette démarche est de comprendre pourquoi une partie des collaborateurs ne s'engage pas dans les campagnes proposées. Les motifs sont rarement ceux que l'on suppose : manque de temps perçu, sentiment d'invulnérabilité, formats jugés inadaptés, défaut de relais managérial, doute sur l'utilité concrète.

Cette information est stratégique : elle indique **sur quels leviers agir prioritairement pour faire progresser la participation**, plutôt que de répéter la même formule en espérant un meilleur résultat.

Notre conviction

« La sensibilisation c'est bien, les résultats c'est mieux. »

PARTIE 4

Mesurer pour piloter : les bons indicateurs

Mesurer une démarche de sensibilisation ne se résume pas à compter les taux de complétion d'un module d'e-learning. Ce dernier est nécessaire mais largement insuffisant pour répondre à l'exigence de diligence. Une mesure crédible mobilise plusieurs familles d'indicateurs, complémentaires.

› Trois indicateurs structurants

Indicateur	Ce qu'il mesure	Pourquoi c'est utile
1 **Niveau de satisfaction**	Perception des supports proposés par les collaborateurs.	Détecter rapidement les contenus mal calibrés et préserver l'adhésion à la démarche.
2 **Montée en compétence perçue**	Progression auto-évaluée par l'apprenant sur les sujets traités.	Valider la valeur pédagogique réelle des modules, au-delà de la simple exposition.
3 **Impact individuel et collectif**	Évaluation, par chaque collaborateur, de l'adoption des bonnes pratiques pour lui-même et autour de lui.	L'écart entre les deux notes est révélateur de la maturité culturelle de l'organisation.

L'écart entre l'impact individuel (« je fais ce qu'il faut ») et l'impact collectif (« mes collègues le font ») est particulièrement instructif. Lorsque le premier est nettement supérieur au second, il révèle un biais classique : **chacun se croit plus vertueux que ses pairs.** C'est un signal qui invite à travailler la norme sociale et le rôle exemplaire du management.

PARTIE 4 (suite)

L'étude d'impact à froid : un dispositif clé

L'étude d'impact à froid consiste à interroger les collaborateurs plusieurs semaines après la fin des campagnes, lorsque l'effet immédiat de la nouveauté est retombé. Elle permet de mesurer ce qui reste réellement ancré, par opposition à un questionnaire de fin de module qui mesure surtout la mémoire courte.

Conduite annuellement, elle offre trois bénéfices majeurs pour le RSSI :

- ✔ Un rapport de pilotage qui suit l'évolution des résultats dans le temps et matérialise la démarche d'amélioration continue.
- ✔ Un support de gouvernance qui permet de faire exister le sujet au niveau du COMEX ou du board, comme l'attend désormais NIS2.
- ✔ Un benchmark externe qui situe les résultats de l'organisation par rapport à un panel global et fournit un étalon de diligence opposable.

De la mesure au pilotage

Mesurer ne sert qu'à condition que le résultat alimente une décision.

Chaque cycle annuel doit donc se conclure par une révision du plan : contenus à renforcer, populations à recibler, formats à diversifier, canaux à activer.

C'est cette boucle, formalisée et tracée, qui constitue la meilleure démonstration de diligence vis-à-vis d'un auditeur ou d'un régulateur.

PARTIE 5

Une méthodologie pour des résultats durables

Mesurer ne suffit pas. Encore faut-il que les actions menées soient effectivement de nature à produire le changement de comportement attendu. C'est tout l'enjeu de la méthodologie pédagogique mise en œuvre. Chez Conscio Technologies, elle s'articule autour de trois grands principes éprouvés.

› Les 4 piliers pédagogiques : Interpeller, Expliquer, Appliquer, Réactiver

Pilier	Objectif	Exemple de moyen
1 **Interpeller**	Susciter l'attention et le questionnement initial du collaborateur.	Campagne de phishing simulée, vidéo d'accroche, témoignage.
2 **Expliquer**	Apporter une compréhension claire des risques et des bons réflexes.	Module e-learning, fiche pratique.
3 **Appliquer**	Faire passer le savoir au comportement par la mise en situation.	Mini-jeu, quizz scénarisé, exercice de signalement.
4 **Réactiver**	Lutter contre l'oubli et inscrire les réflexes dans la durée.	Nudges, rappels ciblés, micro-modules de piqûre de rappel.

› L'approche par les minorités actives

Une partie significative des collaborateurs est intrinsèquement intéressée par les sujets cyber, à condition qu'on leur en donne l'occasion. Repérer, équiper et valoriser ces relais — qu'on les appelle ambassadeurs, champions ou correspondants — produit **un effet d'entraînement bien supérieur à celui obtenu par des campagnes uniformes destinées à tous.**

Cette logique de minorités actives s'inspire des travaux de psychologie sociale qui ont montré qu'un **groupe minoritaire cohérent et persévérant** peut faire évoluer la norme d'un collectif beaucoup plus large.

PARTIE 5 (suite)

La sensibilisation impliquante : engager plutôt qu'informer

La psychologie de la persuasion et de l'engagement nous enseigne qu'un comportement n'est durablement adopté que s'il a fait l'objet d'un acte engageant librement consenti.

C'est le principe de la sensibilisation impliquante : **plutôt que de délivrer un message, on conduit le collaborateur à poser un petit acte** (cocher une option, formuler un engagement, partager une bonne pratique) qui le rend acteur de la démarche.

Plusieurs techniques structurent cette approche : pied dans la porte, étiquetage, inoculation, mobilisation de la dissonance cognitive, rupture du sentiment d'invulnérabilité. Toutes visent le même objectif : **convertir la connaissance en comportement.**

Ce qu'un auditeur NIS2 attend de voir

- Une politique de sensibilisation formalisée et validée par la direction.
- Une couverture des principales thématiques, calibrée selon les profils de risque.
- Des indicateurs de participation ET d'impact, suivis dans le temps.
- Une comparaison avec des organisations comparables.
- Des décisions de pilotage tracées, montrant que la démarche s'adapte aux résultats observés.

PARTIE 6

Check-list : votre dispositif est-il « NIS2-defendable » ?

Cette check-list synthétique permet en quelques minutes d'évaluer la robustesse de votre dispositif au regard de l'exigence de diligence. **Plus le nombre de cases cochées est élevé, plus votre démarche sera défendable en cas de contrôle ou de contentieux.**

GOUVERNANCE ET FORMALISATION

- ❑ Une politique de sensibilisation existe, datée et validée par la direction.
- ❑ Les rôles et responsabilités (RSSI, RH, communication, managers) sont définis.
- ❑ Le sujet remonte au moins une fois par an au COMEX ou au comité des risques.
- ❑ Les choix méthodologiques (cibles, fréquence, canaux) sont documentés et justifiés.

COUVERTURE ET CONTENUS

- ❑ Les thématiques de base sont couvertes (phishing, mots de passe, données, mobilité).
- ❑ Les thématiques émergentes sont intégrées au fil de l'eau (deepfakes, IA, quishing).
- ❑ Les populations à risque élevé (dirigeants, IT, finance, support) bénéficient d'un parcours renforcé.
- ❑ Les nouveaux entrants sont sensibilisés dès leur arrivée.

MESURE ET AMÉLIORATION CONTINUE

- ❑ Les taux de participation et de complétion sont suivis par campagne.
- ❑ Une étude d'impact à froid mesure la satisfaction, la montée en compétence et l'impact perçu.
- ❑ Les freins à la participation sont identifiés et adressés explicitement.
- ❑ Les résultats sont comparés à un benchmark externe (sectoriel ou global).
- ❑ Le plan d'action de l'année N+1 s'appuie explicitement sur les résultats de l'année N.

Moins de 8 cases cochées : votre dispositif présente une exposition juridique réelle face à NIS2.
Entre 8 et 12 cases : vos fondations sont solides, mais quelques angles morts subsistent.
Plus de 12 cases : votre démarche est mature et conforme à l'esprit du devoir de diligence.

À propos de Conscio Technologies

Conscio Technologies est un éditeur français de logiciels spécialisé dans la sensibilisation à la cybersécurité. Basés à Plescop (Morbihan), nous accompagnons **depuis plus de quinze ans des organisations de toutes tailles** — grands comptes, ETI, collectivités, établissements de santé, mutuelles — dans la conception et le pilotage de leurs stratégies de sensibilisation.

› Sensiwave, notre plateforme SaaS

Sensiwave est notre plateforme dédiée. Elle permet à nos clients de déployer leur stratégie de sensibilisation à travers des campagnes de tests de phishing, des parcours e-learning, des actions de communication interne et des dispositifs de mesure d'impact. Elle s'appuie sur une bibliothèque de contenus régulièrement enrichie et sur une méthodologie pédagogique qui place les résultats au centre.

› Notre conviction

« La sensibilisation c'est bien, les résultats c'est mieux. » Au-delà de la fourniture d'un service logiciel, notre engagement consiste à apporter à nos clients les meilleures approches pour obtenir des effets réels sur la participation et l'engagement de leurs collaborateurs.

› Pour aller plus loin

Nous éditons **une collection de livres blancs thématiques** (ETI, sensibilisation impliquante, approches sectorielles) ainsi qu'un ouvrage de référence, « Cybersécurité, l'utilisateur ce héros ».

Si vous souhaitez échanger sur vos enjeux ou découvrir Sensiwave, nous serons heureux d'en discuter avec vous.

Contact :
CONSCIO TECHNOLOGIES
3 Rue Camille Claudel — 56890 Plescop
Téléphone : +33 (**0**)**2 59 50 38 00**
Email : **contact@conscio-technologies.com**
Web : **www.conscio-technologies.com**

Notes

Notes

La sensibilisation c'est bien,
les résultats C'EST MIEUX !

conscio
Technologies

www.conscio-technologies.com