Synthèse de veille réglementaire

Export généré le 06/11/2026 à 03:37 · 10 texte(s) · Les filtres actifs de la page sont conservés.

Textes	10	Action requise	0	À analyser	4	Information	6

À analyser 21/07/2026 · Publication ANSSI · Cybersécurité / Résilience

Exigences du CRA : processus de notification pour les organismes notifiés

Résumé

Exigences du CRA : processus de notification pour les organismes notifiés Publié le mardi 21 juillet 2026 Dans un contexte marqué par l’exploitation croissante de vulnérabilités affectant des produits numériques ayant un niveau de cybersécurité insuffisant, le règlement européen dit « Cyber Resilience Act » (CRA) pendant de NIS 2, permet de développer un marché européen de produits numériques de confiance.Le CRA appelle à un changement d’approche dans la façon de développer et de maintenir nos produits numériques. Pour réussir cette transition, il est indispensable que l’ensemble des parties prenantes collaborent étroitement.Le règlement prévoit également des sanctions pour les entreprises dont les produits numériques mis sur le marché européen ne respecteraient pas les obligations introduites par ce nouveau règlement.Obligations des fournisseurs de produits numériques dans le cadre du C

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

- Lire la publication ANSSI
- Comparer les recommandations aux pratiques du site
- Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 21/07/2026 · Publication ANSSI · Cybersécurité / Résilience

Les actualités : Articles avec l’étiquette Cyber Resilience Act

Résumé

Les actualités : Articles avec l’étiquette Cyber Resilience Act Articles Exigences du CRA : processus de notification pour les organismes notifiés Publié le mardi 21 juillet 2026 CRA, l’ANSSI encourage l’implication d’organismes d’évaluation de la conformité Publié le jeudi 24 juillet 2025 Flux Atom Flux RSS

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

- Lire la publication ANSSI
- Comparer les recommandations aux pratiques du site
- Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

À analyser 06/07/2026 · Publication ANSSI · Cybersécurité / Résilience

L’ANSSI, l’ACPR et la Banque de France signent un accord de coopération

Résumé

L’ANSSI, l’ACPR et la Banque de France signent un accord de coopération Publié le lundi 6 juillet 2026 Les entités du secteur financier sont des cibles privilégiées en raison de la sensibilité des données qu’elles gèrent et des transactions financières qu’elles réalisent.Afin de soutenir le secteur face à la menace cyber, l’Agence nationale de la sécurité des systèmes d’information (ANSSI), l’Autorité de contrôle prudentiel et de résolution (ACPR) et la Banque de France ont signé, le 3 juillet 2026, un accord qui vise à renforcer l’échange d’informations et la coopération dans le respect de la directive NIS 2 et de la règlementation DORA.Dans ce cadre, l’ANSSI conduira les actions nécessaires en matière de réponse technique aux incidents de cybersécurité touchant le secteur financier, via le Centre national et gouvernemental de veille, d’alerte et de réponse aux attaques informatiques (C

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

• Lire la publication ANSSI
• Comparer les recommandations aux pratiques du site
• Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

À analyser 25/06/2026 · Publication ANSSI · Cybersécurité / Résilience

L’ANSSI publie un kit d’exercice de crise pour le secteur agroalimentaire.

Résumé

L’ANSSI publie un kit d’exercice de crise pour le secteur agroalimentaire. Publié le jeudi 25 juin 2026 A l’heure où la menace cyber est omniprésente, les organisations et les entreprises doivent se préparer et réagir rapidement en cas d’attaque informatique afin d’assurer la continuité de leurs activités. Pourtant, l’anticipation et la préparation font encore trop souvent défaut, alors qu’elles s’avèrent essentielles, notamment dans le but de limiter les impacts.Dans ce contexte et alors que tout le monde peut être victime des cyberattaques sans forcément en être la cible, les entités du secteur agroalimentaire ne sont pas épargnées. Pour les accompagner, l’ANSSI met à leur disposition un kit d’exercice qui permet de mieux appréhender l’entraînement à la gestion de crise d’origine cyber et d’aider à la montée en maturité de l’écosystème du secteur dans son ensemble.Ce kit permet de s’ex

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

• Lire la publication ANSSI
• Comparer les recommandations aux pratiques du site
• Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 17/06/2026 · Publication ANSSI · Cybersécurité / Résilience

Publication d’un nouveau référentiel de formation dédié au pilotage de la remédiation

Résumé

Publication d’un nouveau référentiel de formation dédié au pilotage de la remédiation Publié le mercredi 17 juin 2026 La formation au cœur des missions de l’ANSSIA l’heure où le secteur du numérique en général et particulièrement celui de la cybersécurité, connaissent une pénurie de main-d’œuvre à l’échelle mondiale, la capacité de la France à développer et attirer les talents dans les domaines de la cybersécurité apparaît comme un enjeu majeur pour atteindre une résilience cyber de premier rang. Cette ambition constitue l’axe prioritaire au cœur de la stratégie nationale de cybersécurité 2026-2030.Depuis de nombreuses années, l’ANSSI met son expertise et ses moyens à profit pour accompagner le renforcement et l’encadrement de la formation à la cybersécurité afin de répondre aux enjeux et aux besoins évolutifs du secteur.Accompagner l’ensemble des organisations en matière de formationDan

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

- Lire la publication ANSSI
- Comparer les recommandations aux pratiques du site
- Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 16/06/2026 · Publication ANSSI · Cybersécurité / Résilience

Appel à manifestation d‘intérêt – Sécurité des écosystèmes de cybersécurité

Résumé

Appel à manifestation d‘intérêt – Sécurité des écosystèmes de cybersécurité Publié le mardi 16 juin 2026 L'ANSSI ouvre un appel à manifestation d‘intérêt pour le soutien à la création et le développement d’entités chargées de l’accompagnement sectoriel aux enjeux de cybersécurité (AMI SEC), du 16 juin 2026 au 27 juillet 2026. Le présent appel à manifestation d’intérêt définit l’objet du financement envisagé par l’Agence nationale de la sécurité des systèmes d’information (ANSSI) pour encourager les initiatives permettant de renforcer la capacité de coordination sectorielle en matière de cybersécurité au niveau national.En tant qu’autorité nationale en matière de cybersécurité et de cyberdéfense, l’Agence nationale de la sécurité des systèmes d’information prépare et accompagne la montée en maturité cyber de la nation.Dans un contexte où la menace cyber ciblant les entités de certains sec

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

- Lire la publication ANSSI
- Comparer les recommandations aux pratiques du site
- Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 09/06/2026 · Publication ANSSI · Cybersécurité / Résilience

L’ANSSI accompagne les organisateurs dans la cybersécurité du Sommet du G7 à Evian

Résumé

L’ANSSI accompagne les organisateurs dans la cybersécurité du Sommet du G7 à Evian Publié le mardi 9 juin 2026 Dans un contexte de fortes tensions géopolitiques mondiales, la présidence française du G7 en 2026 est exposée à de potentielles attaques informatiques. L’Agence nationale de la sécurité des systèmes d’information (ANSSI) apporte donc son soutien aux organisateurs pour la cybersécurité de l’écosystème associé au Sommet des chefs d’Etat et de gouvernement organisé à Evian du lundi 15 au mercredi 17 juin 2026. L’Agence tient également à rappeler les mesures de prévention et de protection à l’ensemble des parties prenantes au Sommet pour se prémunir contre les cybermenaces.La présidence française du G7 en 2026, et particulièrement le Sommet des chefs d’État et de gouvernement à Evian, représentent une opportunité qui pourrait être exploitée par différents types d’attaquants, aux ni

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

• Lire la publication ANSSI
• Comparer les recommandations aux pratiques du site
• Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

À analyser 21/05/2026 · Publication ANSSI · Cybersécurité / Résilience

Mise à jour du référentiel d’exigences PACS en version 2.0

Résumé

Mise à jour du référentiel d’exigences PACS en version 2.0 Publié le jeudi 21 mai 2026 Le référentiel pour la qualification des prestataires d’accompagnement et de conseil en sécurité des systèmes d’information (PACS) évolue. La nouvelle version du référentiel permet d’adresser un panel plus important de bénéficiaires pour des prestations mieux adaptées à leurs besoins. Les PACS accompagnent les bénéficiaires pour mettre leurs systèmes informatiques en conformité avec des exigences de sécurité spécifiques (LPM, NIS2, etc.) ou pour atteindre un niveau de sécurité déterminé.La qualification d’un prestataire PACS apporte aux bénéficiaires des garanties sur l’impartialité et la compétence du prestataire, la confiance que l’on peut lui accorder et sa capacité à protéger les informations et supports relatifs à la prestation.Les principales modifications apportées par cette nouvelle version son

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

• Lire la publication ANSSI
• Comparer les recommandations aux pratiques du site
• Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 19/03/2026 · Publication ANSSI · Cybersécurité / Résilience

Les actualités : Articles avec l’étiquette Appels à commentaires

Résumé

Les actualités : Articles avec l’étiquette Appels à commentaires Articles L’ANSSI lance un appel à commentaires sur les architectures de référence de sa nouvelle doctrine de supervision de sécurité Publié le jeudi 19 mars 2026 Appel à commentaires sur l’ajout d’un volet gestion de crise au référentiel PRIS Publié le lundi 24 mars 2025 Appel à commentaires sur le vote par internet pour les élections non politiques [CLOS] Publié le lundi 10 mars 2025 Flux Atom Flux RSS

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

- Lire la publication ANSSI
- Comparer les recommandations aux pratiques du site
- Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 28/10/2025 · Publication ANSSI · Cybersécurité / Résilience

Les actualités : Articles avec l’étiquette Visa de sécurité

Résumé

Les actualités : Articles avec l’étiquette Visa de sécurité Articles Publication de la mise à jour du référentiel PRIS en version 3.2 Publié le mardi 28 octobre 2025 Premiers visas de sécurité incluant de la cryptographie post-quantique Publié le jeudi 16 octobre 2025 Appel à commentaires sur l’ajout d’un volet gestion de crise au référentiel PRIS Publié le lundi 24 mars 2025 L’ANSSI met à jour les référentiels PASSI (version 2.2) et PRIS (version 3.0) Publié le vendredi 29 novembre 2024 Flux Atom Flux RSS

Impact pour l’exploitant
Doctrine ou recommandation ANSSI pouvant intéresser la résilience des systèmes utilisés pour l'exploitation, la sûreté ou la gestion de crise.

Actions recommandées

- Lire la publication ANSSI
- Comparer les recommandations aux pratiques du site
- Identifier les écarts utiles à intégrer dans les plans de sécurité ou de continuité

Entrée en vigueur : Non précisée

Ouvrir la source officielle