

Formation pilotage de la sécurité des SI en ESMS

Contexte de formation

Cette formation a pour objectif de mettre à niveau les RSSI et chefs de projet SSI sur la cybersécurité en santé.

Cette formation est animée par l'APSSIS et dure 2 jours. Elle aborde :

- le contexte et les cadres institutionnels, réglementaires, technologiques qui régissent la sécurité des SI de santé,
- La gouvernance et le pilotage de la SSI.

Une formation originale produite par Vincent Trely, Président de l'APSSIS et Pascal Sabatier, RSSI et DPO du GHT 04 et du Centre Hospitalier d'Aix-en-Provence

Objectifs de la formation

- Connaître l'ensemble des **politiques et cadres réglementaires** de la sécurité des SI de santé.
- Elaborer **un plan d'actions** SSI cohérent;
- Mettre en œuvre une **gouvernance et un pilotage** de la sécurité des SI.



Date et durée

25 et 26 septembre 2025
(formation de 2 jours)
de 9h à 17h00



Lieu

Montpellier



Public concerné

RSSI
Chef de projet SSI en santé

Programme

Jour 1.

Cyber insécurité –
Impacts sur les systèmes
de santé – Actualités –
Environnement
réglementaire UE et
France – Programmes
d'État

Jour 2.

Produire, piloter et
promouvoir le plan
d'action SSI

Programme détaillé : jour 1

Cyber insécurité – Impacts sur les systèmes de Santé – Actualités – Environnement Réglementaire UE & FR – Programmes d’Etat

9h00 : Accueil – Présentation de l’organisation de la formation – Tour de table et présentation

9h30 : Contexte international et national de l’insécurité numérique

Typologie des menaces et des acteurs – Etat des lieux – Chiffres – Données – Actualité internationale

Cas particulier du système de santé – Criticité des SI de santé – Impacts des cyber attaques

11h15 : Environnement institutionnel, réglementaire et normatif de la cybersécurité en santé - I

Les nouveaux enjeux de la SSI santé – La Cybersécurité des établissements de santé : une priorité nationale

Gouvernance de la SSI Santé : UE, Etat, ANSSI, Ministère, DNS, DGOS, ANS, ARS, GRADeS, GHT, Etablissements publics et privés, ESMS

RGPD – Directive NIS II – Autres textes : Cloud, Données, Plates-formes, Souveraineté

PSSI-MCAS, PGSSI-S, **43 mesures prioritaires et Programme CaRE**

Référentiel MATURIN-H pour les établissements sociaux et médico-sociaux

12h30 : Déjeuner

14h00 : Environnement institutionnel, réglementaire et normatif de la cybersécurité en santé - II

Référentiels et Guides – Méthodes et état de l’art de la SSI

Analyses des risques : méthodes EBIOS RM, transition méthodologique – Analyses des risques métiers

Directive NIS applicable aux OSE (EE et EI) – Textes, détail des règles de sécurité

Certification ISO 27001 – Certification HDS II – Enjeux, objectifs, méthodes

15h45 : Veille technologique et stratégique

Cloud – Intelligence artificielle – Identité numérique – Projets UE et FR

Certifications et labels – Veille juridique sur les usages

17h00 : fin de la première journée

Programme détaillé : jour 2

Jour 2 : Produire, piloter et promouvoir le plan d'action SSI

9h00 : Accueil – Présentation de la journée – Synthèse J1

9h15 : Gouvernance et pilotage de la SSI - I

Rôle et responsabilités des acteurs : RSSI, Référent SSI, DPO, Directions, Métiers

Transformer un / des référentiel(s) en plan d'action opérationnel

PSSI et documents socles (chartes utilisateurs et administrateurs, politiques spécifiques, comitologie)

Plan de traitement des risques – Programme de sensibilisation – Programme de contrôle et d'audit – Plan projets => **Plan d'action SSI**

Analyse et transformation des mesures prioritaires de sécurité – Politiques, procédures, instructions, documents

11h15 : Gouvernance et pilotage de la SSI - II

Gouvernance SSI des établissements de santé : cartographies des risques, pilotage et budget

Diagnostic et maîtrise des SI : cartographies des actifs et des flux, audits techniques et d'organisation

Sécurisation et mise en conformité : mesures techniques et coopération avec les parties prenantes (Métiers, Directions)

Sensibilisation des professionnels aux risques cyber

12h30 : Déjeuner

14h00 : Gouvernance et pilotage de la SSI - III

Anticipation et réponse aux incidents cyber – PRA et PCA métiers

Gestion des incidents – Déclaration des incidents – Gestion de crise cyber

Intégration de la SSI dans les projets - Indicateurs de sécurité du RSSI et modalités de communication

15h45 : EVALUATIONS

Réalisation de l'évaluation fonctionnelle

Réalisation de l'évaluation qualité

16h45 : Synthèse finale et questions / réponses

17h00 : fin de la formation