Sécurité des Systèmes d'Information

Protection des données

Pourquoi et comment
AGIR DÈS AUJOURD'HUI

TESIS
E-SANTÉ

LE PITCH !

pour tout comprendre en une minute

CYBERSÉCURITÉ RISQUE IMMÉDIAT, CONSÉQUENCES GRAVES

Le secteur santé traverse une crise cyber durable. Des dizaines d'établissements sont touchés chaque année par des attaques informatiques qui peuvent paralyser les infrastructures techniques et stopper l'activité. Les dégâts se chiffrent alors en millions d'euros, mais surtout en vies humaines.
En cause : le manque de préparation et d'anticipation, et les défauts de conformité des structures de santé.

RÉPONDRE À VOS BESOINS URGENTS

Dans ce contexte, le GCS TESIS lance une offre régionale pour aider vos établissements à assurer la sécurité des SI (SSI) et protéger les données personnelles de vos employés et usagers (PDP).

UNE OFFRE À LA CARTE

Choisissez votre mode d'accompagnement : intervention ponctuelle **ou** régulière sur 3 ans dans le cadre d'un plan de mise à niveau.

MUTUALISATION ET MAÎTRISE DES COÛTS

Une démarche régionale pour renforcer la cohérence de vos actions et diminuer l'impact financier pour vos structures :

INTERVENTION DU GCS TESIS :
→ Accompagnement par le GCS TESIS chiffré au temps passé, facturé à prix coûtant.

CATALOGUE DE PRESTATIONS EXTERNALISÉES
→ Prestations ponctuelles externalisées à tarifs négociés grâce aux procédures de marché simplifiées du GCS.

APPROCHE GLOBALE DES RISQUES

Nous couvrons l'ensemble des vulnérabilités et des obligations légales : audit, détection des failles, gouvernance, gestion des incidents, plans de continuité mais aussi formation- sensibilisation professionnelle et information usagers.

LES MEILLEURES INNOVATIONS DU MARCHÉ

Retrouvez sur catalogue des services spécialisés pour maximiser l'engagement et la sensibilisation de vos équipes (campagnes de phishing, e-Learning), mais aussi des prestataires solides pour vous épauler dans la gestion des incidents.

ACCOMPAGNEMENT PERSONNALISÉ

Nous partons de vos besoins et de votre maturité pour dimensionner toutes nos interventions. **Vous ne payez que le nécessaire.**

UN PÔLE D'EXPERTISE SSI & PDP

Coordonnée par le RSSI Régional, l'équipe Cybersécurité du GCS TESIS s'appuie sur des profils experts internalisés, formés spécialement aux enjeux des SI santé.

Nos experts peuvent :

→ **intervenir ponctuellement dans vos structures,**

→ **accompagner vos établissements dans la durée,**

→ **exercer les fonctions RSSI et DPD pour votre compte.**

Quel est le prix de votre sécurité ?

Prenons rendez-vous !

Mathias Laurent,
Responsable Régional de la Sécurité des Systèmes d'Information en Santé, est à votre disposition pour évaluer vos besoins.

m.laurent@tesis.re

06 93 93 37 35

Sommaire

TESIS
E-SANTÉ

La sécurité des systèmes d'information et le respect des règles de confidentialité sont au cœur de nombreux enjeux pour les structures sanitaires et médico-sociales, quelle que soit leur taille.

Garantir la qualité et la sécurité des soins et de l'accompagnement aux usagers

Améliorer les conditions d'exercice des professionnels de santé

Assurer votre conformité légale et réglementaire

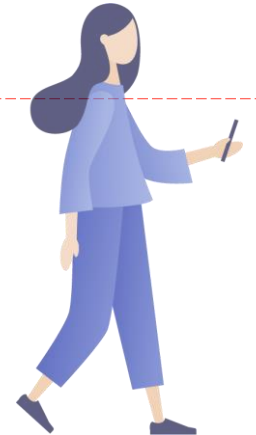
Vous prémunir de potentielles attaques, d'origine interne ou externe

Préserver vos ressources financières

Maintenir l'efficacité et la continuité opérationnelle de vos structures

Protéger la vie privée de vos employés, fournisseurs, partenaires et usagers

Protéger votre image et votre notoriété



Sécurité des Systèmes d'Information

Protection des données

Pourquoi est-ce le moment d'agir ?

TESIS
E-SANTÉ

1. Le risque cyber est critique dans le secteur santé

Plus de 150 attaques par des rançongiciels ont frappé avec succès des établissements français depuis 2018, et les chiffres augmentent chaque année.

La menace atteint aujourd'hui un seuil critique, et peut être considérée comme immédiate.

Lorsqu'elles frappent des structures mal préparées, ces attaques ont de lourdes conséquences sur la prise en charge des usagers : arrêt de l'activité, indisponibilité des services informatiques, des plateaux techniques, de la climatisation…

Les impacts sont dévastateurs :

- Dégradation des prises en charge
- Pertes financières
- Image dégradée (ces attaques font l'objet d'une plus grande couverture médiatique)
- Etc.

2. Vos obligations légales deviennent opposables

La Politique Générale de Sécurité des Systèmes d'Information dans la Santé (PGSSI-S) et la Politique de sécurité des systèmes d'information des Ministères Sociaux (PSSI-MCAS) sont aujourd'hui opposables aux établissements de santé. Ils vous obligent à :

→ Mettre en place une gouvernance SSI

→ Gérer les risques SSI

→ Protéger les données et les systèmes

→ Sensibiliser et former la totalité des personnels

→ Auditer les vulnérabilités du SI

→ Gérer les incidents SSI

→ Sécuriser l'Identification et l' l'Authentification des acteurs

Certains de ces points ont fait l'objet d'un rappel dans le Message d'Alerte Rapide Sanitaire (MARS) du 6 avril 2021, adressé aux structures ultramarines**. D'autres font désormais partie des objectifs inscrits en annexe de vos CPOM avec l'ARS La Réunion.**

3. Un levier pour vos financement en matière de numérique

Dans le cadre du Ségur de la Santé et du Plan Ma Santé 2022, vos établissements peuvent financer la mise à niveau et le renouvellement d'équipements informatiques, et les travaux nécessaires pour s'inscrire dans la Doctrine Technique du Numérique en Santé.

Pour être éligible aux programmes suivants, vous devez remplir vos obligations en matière de cybersécurité et de protection des données :

→ HOP'EN

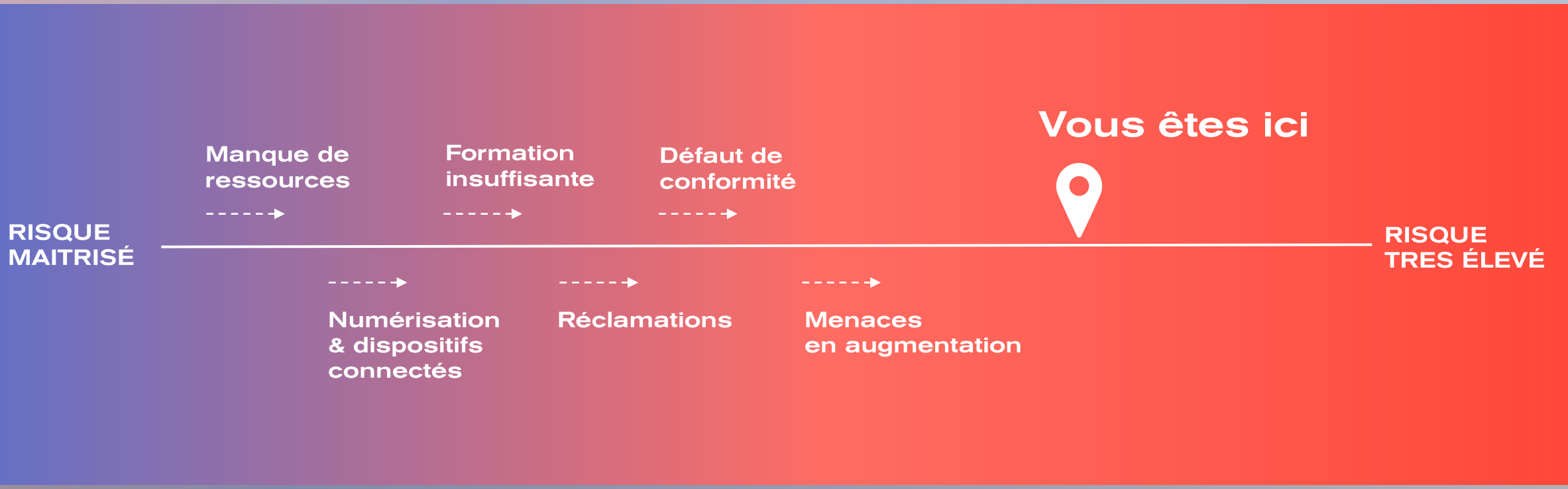
→ SUN-ES

→ ESMS Numériques

Pour y voir clair

Liste complète des obligations et prérequis en annexe, p.25

L'accumulation des failles rend vulnérables les structures de santé. Sans action de votre part, le risque augmente et les conséquences d'un incident deviennent plus graves.



Sécurité des Systèmes d'Information

Protection des données

Comment TESIS vous accompagne

TESIS
E-SANTÉ

NOTRE APPROCHE

Une démarche régionale mutualisée portée par le GCS TESIS, soutenue par un catalogue de prestations externalisées

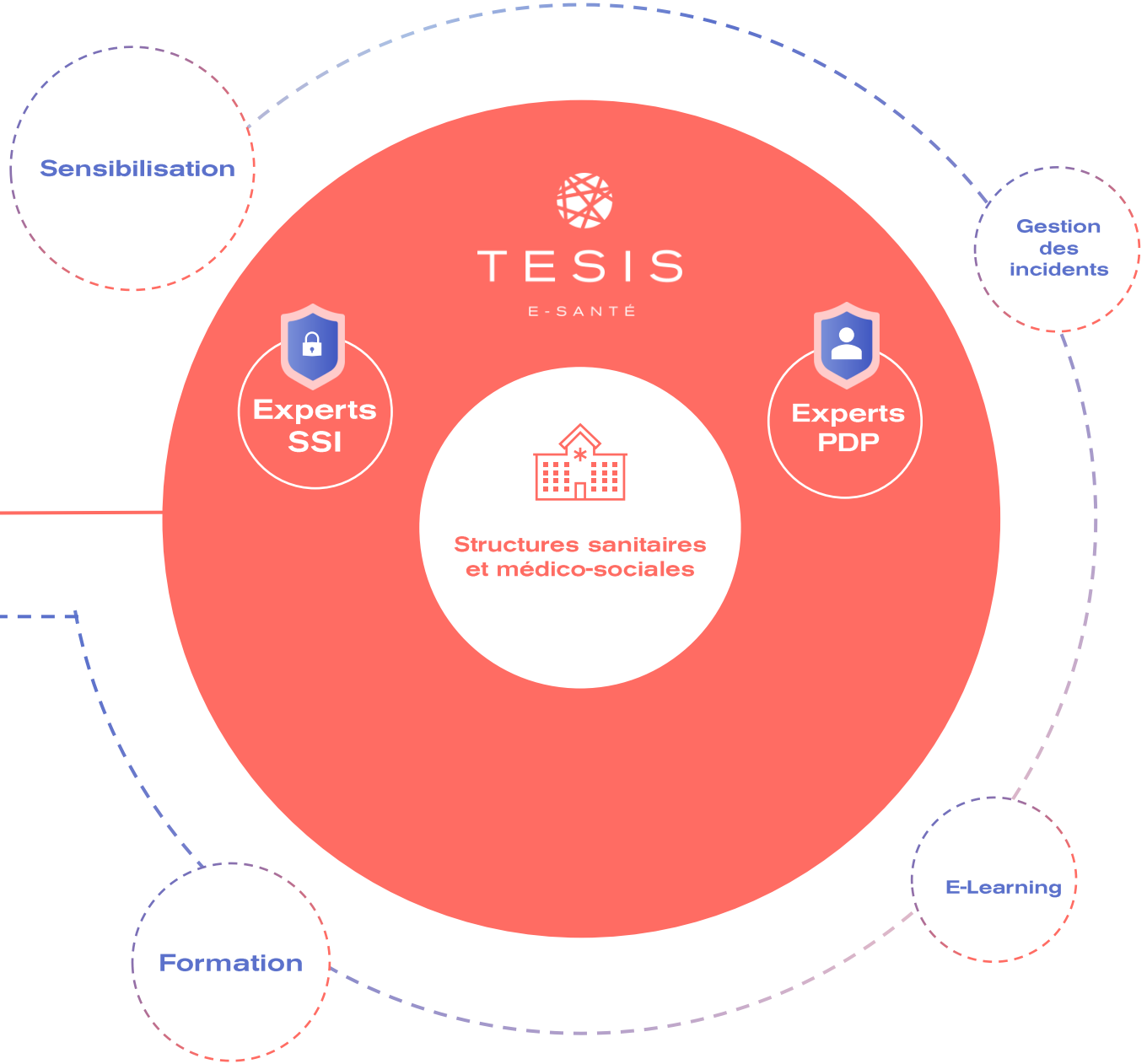
Intervention du GCS TESIS

Un pool **d'experts** internalisé (RSSI, DPD) peut intervenir dans vos structures, ponctuellement ou dans le cadre d'une mise à disposition, à prix coûtant.

Externalisé

Délégation des **prestations** spécialisées (sensibilisation, gestion des incidents) grâce aux marchés du GCS TESIS

Mutualisation des coûts pour les adhérents



NOS SERVICES

Intervention du GCS TESIS

Accompagnement assuré par les équipes du GCS TESIS

Missions ponctuelles

Sécurité des Systèmes d'Information

- Audit de maturité
- Audit et Plan de Contrôle
- Analyse de risques
- Gouvernance
- Documentation
- Cadrage et suivi des projets

Conformité RGPD & DPD

- Audit de maturité
- Conformité RGPD et documentation
- Information et droits des usagers
- Gestion des sous-traitants
- Analyse d'impact
- S.O.S DPO !

Offres packagées

Plan SSI

3 ans pour structurer votre sécurité

Plan RGPD & PDP

3 ans pour organiser votre gestion des données personnelles

Ressources dédiées

Votre RSSI externalisé

Votre DPD externalisé

Externalisé

Prestations externalisées via les marchés souscrits par le groupement

Prestations et outils sur catalogue

Gestion des incidents

- Prévention et détection
- Gestion de crise
- Réponse aux incidents de sécurité

Formation & sensibilisation

- Escape game (Médiscape)
- e-Learning & campagne de phishing
- Evènements de sensibilisation

TESIS E-SANTÉ

PLAN D'ACCOMPAGNEMENT SSI

3 ANS POUR STRUCTURER VOTRE SÉCURITÉ

Objectifs :

Réduire rapidement votre risque cyber en vous dotant de l'organisation et des moyens pour faire face aux attaques.

Remplir vos obligations réglementaires en matière de SSI, prérequis aux programmes nationaux HOP'EN, SUN-ES et ESMS Numériques.

Première année

Vous protéger en cas d'attaques

- ❑ AUDIT
- ❑ MISE EN PLACE D'UNE GOUVERNANCE INTERNE
- ❑ PLAN DE TRAITEMENT D'URGENCE :
  - Gestion d'incident
  - Socle de sécurité opérationnelle
  - Sensibilisation
  - Plan de Continuité Informatique (PCI)
  - Plan de Reprise Informatique (PRI)

Deuxième année

Identifier vos failles et renforcer votre sécurité

- ❑ ANALYSE DES RISQUES CRITIQUES
- ❑ CONSTRUIRE VOTRE SECURITE A LONG TERME
  - Gestion des identités et des accès
  - Gestion des actions d'administration
  - Sécurité des réseaux
  - Gestion des sous-traitants – Homologation des projets
  - PCI / PRI de niveau 2

Troisième année

Améliorer votre performance globale

- ❑ REVUE ET EXTENSION DE L'ANALYSE DE RISQUES
- ❑ CONSOLIDATION ET SUIVI DES MESURES MISES EN ŒUVRES AUX NIVEAUX 1 ET 2

+ AU BESOIN

commande de prestations externalisées

PLAN D'ACCOMPAGNEMENT RGPD & PDP

3 ANS POUR ORGANISER LA PROTECTION DES DONNÉES PERSONNELLES

Objectifs :

Réduire rapidement votre risque face à un défaut de conformité RGPD.

Remplir vos obligations réglementaires en matière de PDP, prérequis aux programmes nationaux HOP'EN, SUN-ES et ESMS Numériques.

Première année

Vous doter d'un socle minimal de conformité au RGPD

- ❑ AUDIT DE MATURITE
- ❑ MISE EN PLACE D'UNE GOUVERNANCE INTERNE
- ❑ MISE EN PLACE DU REGISTRE
- ❑ PLAN DE TRAITEMENT D'URGENCE : (sur les traitements les plus sensibles)
  - Gestion de l'information et droits des personnes concernées
  - Analyse d'impact
  - Sensibilisation
  - Gestion de la contractualisation avec les sous-traitants

Deuxième année

Mettre en œuvre vos actions de conformité

- ❑ SENSIBILISATION
- ❑ INFORMATION ET GESTION DU CONSENTEMENT DES TRAITEMENTS
- ❑ 2e NIVEAU DE MESURES EN PRIORITE SUR LES TRAITEMENTS LES PLUS SENSIBLES
  - Gestion des droits des personnes concernées
  - Analyse d'impact
  - Gestion des sous-traitants
  - Notification des incidents

Troisième année

Améliorer votre gestion de la conformité RGPD

- ❑ AUDIT DES MESURES MISES EN PLACE
- ❑ CONSOLIDATION DES MESURES MISES EN PLACE AUX NIVEAUX 1 ET 2
- ❑ EXTENSION AUX AUTRES TRAITEMENTS

+ AU BESOIN

commande de prestations externalisées