RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

CYBERSÉCURITÉ : PROTÉGER LES ÉTABLISSEMENTS DE SANTÉ AVEC FRANCE RELANCE

Le 3 septembre 2020, le Gouvernement annonce un plan de relance national pour redresser durablement l'économie. Avec un fonds de 136 millions d'euros spécialement dédié à la cybersécurité et piloté par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le plan France Relance prévoit de renforcer le niveau de cybersécurité des administrations, des collectivités et des organismes au service des citoyens, tout en dynamisant l'écosystème industriel français.

LES ÉTABLISSEMENTS DE SANTÉ, UNE PRIORITÉ DU VOLET CYBERSÉCURITÉ DE FRANCE RELANCE

Face à la forte augmentation des cyberattaques dans ce secteur, il devient indispensable et urgent d'accroître le niveau de sécurité des établissements de santé afin qu'ils continuent d'assurer pleinement leurs missions quotidiennes au service de nos concitoyens et protègent les données médicales.

Pour cela, l'État déploie *via* France Relance des moyens inédits dédiés à ce secteur pour financer des prestations et des produits de cybersécurité au profit des acteurs de la santé.

Le volet cybersécurité de France Relance se fonde sur l'implication et le volontariat de ses bénéficiaires. Il donne accès à un accompagnement adapté au niveau de maturité et aux enjeux de chaque établissement de santé.

QUI PEUT EN BÉNÉFICIER ?

Le volet cybersécurité de France Relance bénéficie au plus grand nombre d'établissements de santé. Il entend toutefois cibler en priorité les établissements principaux des groupements hospitaliers de territoire (GHT). Les objectifs ? Concentrer l'effort sur des systèmes d'information bénéficiant à plusieurs entités et permettre à chacun de ces groupements de capitaliser sur la démarche en diffusant auprès de l'ensemble de ses membres les bonnes pratiques de cybersécurité.

RENFORCER LA SÉCURITÉ DE SON ÉTABLISSEMENT GRÂCE AUX PARCOURS DE CYBÉRSECURITÉ

L'ANSSI propose aux établissements de santé une offre de « **Parcours de cybersécurité** ».

Elle leur permet, après un diagnostic cyber, de se mettre à niveau, notamment au travers de la sensibilisation et de la formation, et de déployer un ensemble de mesures organisationnelles et techniques de cybersécurité.

4 niveaux de parcours sont proposés : **Fondation** / **Intermédiaire** / **Avancé** / **Renforcé**.

DES OBJECTIFS EN ADÉQUATION AVEC LE NIVEAU DE MATURITÉ DE CHACUN

Les Parcours de cybersécurité ont pour objectif de permettre aux bénéficiaires de se protéger face aux menaces cybercriminelles de masse notamment et de pouvoir les contrer. Chaque parcours permet d'atteindre un objectif de cybersécurité de façon progressive, mesurable et adaptée à chaque établissement.

La mise en œuvre de cette offre se décline en 3 étapes :

- un **pré-diagnostic**, pour orienter le bénéficiaire vers le parcours le plus adapté ;
- une **phase initiale**, afin de mettre en place de premières mesures de sécurisation et d'élaborer une **feuille de route complète de renforcement de la cybersécurité** ;
- un ou plusieurs **accompagnements complémentaires**, afin d'approfondir certaines actions de sécurisation et déployer des solutions de sécurité.

Les travaux déjà entrepris par les établissements en matière de cybersécurité seront pris en compte dans la phase initiale, afin d'accélérer l'élaboration de la feuille de route et de capitaliser sur les actions déjà accomplies.

QUEL FINANCEMENT ?

Le financement des prestations qui composent les Parcours de cybersécurité s'effectue au travers de subventions directes aux établissements de santé principaux de GHT. Dans tous les cas, un co-financement par le bénéficiaire est demandé.

À l'issue du parcours, il est essentiel que chacun pérennise son investissement dans la cybersécurité, *a minima* à hauteur de 5 % de son budget informatique.

En savoir plus et candidater : **www.ssi.gouv.fr/FranceRelance**

SOUTENIR LE DÉVELOPPEMENT DE LA CELLULE **ACCOMPAGNEMENT CYBERSÉCURITÉ DES STRUCTURES DE SANTÉ** (ACSS)

Le volet cybersécurité de France Relance se traduit également par la mise en place d'un accompagnement technique, méthodologique et financier au profit de la cellule **Accompagnement cybersécurité des structures de santé** (ACSS) du ministère des Solidarités et de la Santé.

Avec le soutien de l'ANSSI, l'ACSS a récemment rejoint le **réseau national des centres de réponse à incident**.

Son rôle est notamment de renforcer le suivi des incidents cyber affectant les établissements de santé et d'alerter les acteurs sectoriels lorsqu'une menace voit le jour.

En savoir plus sur l'ACSS : **www.cyberveille-sante.gouv.fr**

Pour tout savoir sur le volet cybersécurité de France Relance : www.ssi.gouv.fr/FranceRelance

---

Version 1.0 – Avril 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr