Guide de la CYBER SÉCURITÉ pour les DIRECTEURS ET DIRECTRICES d'établissement de santé

TOUS CYBER VIGILANTS

Version mars 2025 - réalisé par SESAN

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

sesan
Groupement d'Intérêt Public eSanté

5 Questions à se poser

Qui est responsable de la sécurité du Système d'Information de mon établissement ?

1

La direction générale est responsable de la sécurité du système d'information (SSI) et doit désigner un responsable ou un référent SSI.
Ce dernier peut faire partie du personnel de l'établissement ou être un prestataire externe

Comment organiser la gouvernance SSI de mon établissement ?

2

Au moins deux fois par an, le RSSI et le responsable PCA doivent présenter à la direction et à la Commission Médicale d'Établissement :

- Un bilan SSI
- Le plan d'actions et le budget SSI
- L'actualité SSI
- Les évolutions réglementaires SSI
- La cartographie des risques numériques de l'organisation

Mon établissement est-il préparé à faire face à une cyberattaque ?

3

Un Plan de Continuité et de Reprise d'Activité (PCRA) est essentiel pour que tous les membres de votre personnel puissent maintenir les activités essentielles de votre organisation en cas de perte totale du Système d'Information. Afin d'être bien préparé, des exercices de Cybercrise et des tests du PCRA (dans chaque service) doivent être réalisés régulièrement. La direction générale est responsable de l'élaboration et du pilotage du PCRA, avec l'appui du responsable PCA qu'elle désigne. Celui-ci est issu en interne du service qualité ou de la communauté des soins, ou peut être un prestataire externe

4

Comment financer ma Cybersécurité ?

Certaines actions, comme la sensibilisation du personnel à la cybersécurité, ne nécessitent pas d'investissement majeur.
De plus, chaque année, des programmes régionaux et nationaux (exemple : CaRE) vous permettent de financer une partie des actions d'hygiène informatique.
https://esante.gouv.fr/strategie-nationale/cybersecurite

https://cyberservices.sante-idf.fr/

Quelles sont mes obligations en cas d'incident cyber ?

5

En cas d'incident cyber, je dois obligatoirement réaliser un signalement auprès du CERT Santé (article L1111-8-2 du code de santé publique).
Si l'incident implique une violation de données personnelles (perte de disponibilité, d'intégrité ou de confidentialité, de manière accidentelle ou illicite), je dois le notifier à la CNIL dans les meilleurs délais, au plus tard dans les 72 heures.

Quels sont les IMPACTS et les A
en cas de CYBERATTAQUE

LES PREMIERS JOURS/ LE PREMIER MOIS

- Perte de données : perte de disponibilité et d'intégrité des sauvegardes
- Désorganisation des services et des flux de patients
- Nécessité de déprioriser les prises en charge et de transférer des patients, en lien avec l'ARS
- Mise en place de procédures dégradées dans tous les services touchés (notamment les plateaux techniques, la pharmacie)
- Fermeture temporaire de certains services (le plus souvent, les urgences)
- Impossibilité ou difficulté à facturer et recevoir les paiements
- Renfort nécessaire des équipes soignantes et administratives/ heures supplémentaires
- Arrêt des canaux de communication (internet)

- Renfort nécessaire des équipes / heures supplémentaires
- Investigation, sollicitation de prestataires experts

- Déclaration obligatoire de l'incident au CERT Santé
- Sollicitation de prestataires experts
- Installation cellules de crise et coordination avec l'ARS
- Dépenses imprévues (prestations, heures supplémentaires, matériels…)

- Sollicitation de prestataires expert en communication de crise
- Mise en place d'une communication de crise, interne et externe

- Gestion des éventuelles plaintes des personnes concernées
- En cas de violation de données personnelles, déclaration de l'incident à la CNIL dans les 72 heures

ACTIONS à mener

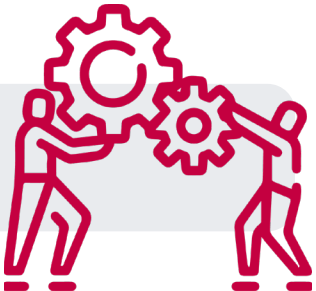
LES MOIS SUIVANTS/ LES ANNÉES SUIVANTES

- Mise en place d'un projet de retour à la normale qui peut durer plusieurs mois, accompagné de ressources dédiées
- Retour partiel à un fonctionnement normal
- Difficulté à facturer et recevoir les paiements
- Reprise des données vers le nouveau Système d'Information

- Renfort nécessaire des équipes Système d'Information
- Reconstruction du Système d'Information
- Déploiement de solutions complémentaires de sécurité

- Maintien de la cellule de crise jusqu'à la reconstruction totale du système d'information

- Reconstruction de l'image de l'établissement
- Communication vers les personnes concernées (en cas de fuite de données)



- Suite judiciaire
- Amendes éventuelles

Quelques événements et chiffres clés

EN 2022, UNE CYBERATTAQUE DANS UN ÉTABLISSEMENT FRANCILIEN A EU COMME RÉPERCUSSIONS :

10 millions d'euros

De demande de rançon réclamée par les hackers

7 millions d'euros

Coût estimé de la cyberattaque (2 millions pour la gestion de la crise et 5 millions pour la reconstruction de l'infrastructure informatique), sans compter les coûts de perte d'exploitation liés à l'arrêt momentané de tout ou partie de l'activité

581

nombre d'incidents déclarés en 2023 au **CERT-SANTÉ**

50 % des incidents

déclarés sont d'origine malveillante

Mon établissement est-il concerné ?

La cybercriminalité est une activité rentable et très organisée.
De plus, les établissements ont une dépendance de plus en plus grande au numérique et les données qu'ils traitent sont sensibles (et donc rémunératrice).
Notre secteur est devenu très attractif aux yeux des cybercriminels.

Que ce soit une attaque opportuniste ou une attaque ciblée, aujourd'hui, aucun établissement n'est à l'abri !

LEXIQUE

RSSI
Responsable de la Sécurité du Système d'Information

RPCA
Responsable du Plan de Continuité d'Activité

CERT-SANTÉ
Cellule de veille, d'alerte et de réponse

ANSSI
Agence Nationale de la Sécurité des Systèmes d'information

CNIL
Commission Nationale de l'Informatique et des Libertés

GRADeS
Groupement Régional d'Appui au Développement de l'eSanté

SSI
Sécurité des Systèmes d'Information

VOS INTERLOCUTEURS

SESAN
GIP SESAN, GRADeS de l'Ile-de-France
Contact: ssi@sesan.fr
Site web : https://cyberservices.sante-idf.fr/

CERT SANTE – Cyberveille Santé
Pour déclarer vos incidents : https://signalement.social-sante.gouv.fr
Allez dans la rubrique «Vous êtes un professionnel de santé»
Tel : 09 72 43 91 25 (24h/24 7j/7)
Contact : cyberveille@esante.gouv.fr

CNIL
Téléservice de notification d'une violation de données personnelles :
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

POUR ALLER PLUS LOIN

Ministère du Travail, de la santé, de la solidarité et des familles
Dossier Cybersécurité :
https://sante.gouv.fr/systeme-de-sante/e-sante/sih/dossier-cybersecurite/

Instruction n°DNS/2025/12 du 22 janvier 2025
relative à l'obligation de mettre en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaires :
https://sante.gouv.fr/fichiers/bo/2025/2025.3.sante.pdf#page=57

Agence Nationale de Sécurité des Systèmes d'Information
Recommandations nationales :
https://www.ssi.gouv.fr/administration/bonnes-pratiques/

Secteur de la santé, État de la menace informatique
https://cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-010.pdf

CNIL
Recommandations nationales :
https://www.cnil.fr/fr/sante