Financé par l'Union européenne
NextGenerationEU

Renforcement de la cyber sécurité dans les établissements sanitaires

Réunion ARS Ile-de-France / SESAN

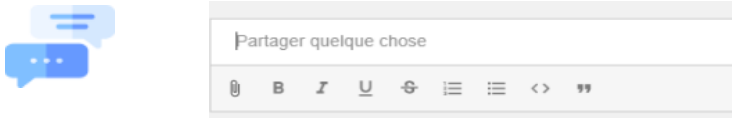
18 septembre 2023

Informations pratiques

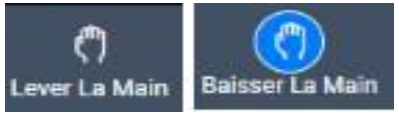
Bonnes pratiques de participation au webinaire

- Je coupe mon micro et ma caméra quand je ne parle pas

- Les questions doivent être posées par écrit, j'utilise le chat en bas de l'écran pour rebondir, poser mes questions ou commenter. Une réponse concise/synthétique sera effectuée à l'oral. Si besoin un retour dédié sera fait par email ou par une prise de contact.



- Si vous souhaitez compléter oralement, levez la main et la parole vous sera donnée.



Mise en ligne de l'enregistrement vidéo de la session : suivez le lien fourni ultérieurement

Ordre du jour

Contexte

Contexte

Incidents SI Santé – les impacts

Les attaques cyber sur les établissement de santé sont de plus en plus nombreuses, et les attaques réussies aussi.

Contexte JO = risque élevé de cyberattaque pour déstabiliser, désorganiser, décrédibiliser

Contexte international : Guerre Ukraine, autres menaces diverses

Les incidents cyber peuvent avoir des impacts très lourds pour les établissements :

- Risques sur la **prise en charge des patients** : indisponibilité des outils métier, des plannings, des coordonnées des personnels et des patients, du logiciel de paie, des moyens de communication internes, etc.
- Un **retour à la normal qui peut être très long et coûteux** : parfois nécessité de reconstruire le SI, y compris sans chiffrements des données (cf. 7ième colloque cyber au ministère de la santé) ;
- Risque de fuite de données et donc **risque juridique** majeur pour l'établissement et son responsable de traitement ;

En cas d’attaque réussie

Rappel de la procédure

En cas d’attaque réussie il faut immédiatement :

- **Pour les établissements non OSE : déclarer l’incident au CERT SANTE** afin de déclencher l’aide du CERT et/ou de l’ANSSI : 09 72 43 91 25, permanence 7j/7, 24h/24, https://signalement.social-sante.gouv.fr

- **Pour les OSE, déclarer l’incident à l’ANSSI** : Téléphone. +33 (0)1 71 75 84 68 : permanence 7j/7, 24h/24.

- En cas de suspicion ou fuite avérée de données, il faut réaliser un **signalement auprès de la CNIL** dans les 72 heures, dans la rubrique : notifier une violation de données personnelles | CNIL

Contexte

SEGUR & Plan de Renforcement Cyber : les attentes envers les ES

1. Réalisation une fois par an d'un **exercice de continuité d'activité en mode numérique dégradé**

2. Réalisation annuelle d'**audits ADS, Silene et de cybersurveillance** (obligatoire pour les OSE, fortement recommandés pour tous)

3. Mise à jour de l'**observatoire (OPSSIES)**

4. **Sensibilisation** des personnels (*en particulier, respecter les consignes des autorités judiciaires durant la crise*)

5. **Avoir une cartographie** la plus exhaustive possible (applicative, réseau…)

6. **Task force Nationale** : plan d'action cyber sur 5 ans selon 4 volets : gouvernance ; ressources et mutualisation ; sécurité opérationnelle ; sensibilisation et devant aboutir fin **juin 2023** pour le plan de financement (plan de financement annuel, RH, licences…) avec en particulier des appels à projets sur les thématiques prioritaires : **postes de travail et détection, Active Directory, passerelles pour les accès des prestataires, sauvegardes**

7. **Groupe de travail régional cyber-résilience** chargé de définir les actions régionales de prévention, gestion de crise et reconstruction

Focus sur les exercices de continuité d'activité

Les kits d'exercice de cybercrise de l'ANS

Objectifs

1. Découvrir la gestion de crise cyber en condition réelle dans le contexte de votre établissement de santé
2. Comprendre l'écosystème cyber de votre structure
3. Adopter les bons réflexes en situation de crise cyber
4. Assurer au mieux la continuité des soins

Les kits d'exercice de cybercrise de l'ANS

3 niveaux

1. Débutant
2. Intermédiaire
3. Confirmé

Les kits d'exercice de cybercrise de l'ANS

Quel est le kit qui me correspond ?

- Grille d'auto-évaluation :
  - ➢ Une fiche d'identité à compléter
  - ➢ Une liste de 23 questions (case à cocher)
  - ➢ Une grille d'appréciation des résultats

Les kits d'exercice de cybercrise de l'ANS

Exemple de question

Score

< 75 : kit débutant

74 < Score < 151 : kit intermédiaire

> 150 : kit confirmés

- Grille d'auto-évaluation

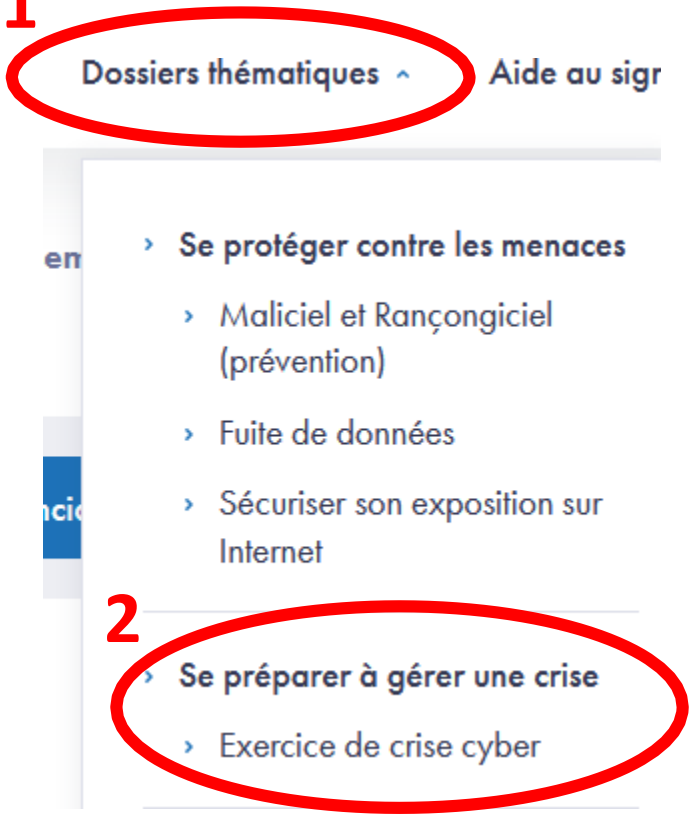
Question	Kit débutants		Kit intermédiaires		Kit confirmés	
Comment les utilisateurs à privilèges sont-ils recensés ? Sont-ils informés de leurs rôles et responsabilités en matière de cybersécurité ?	- Les utilisateurs à privilèges sont recensés de manière informelle - Les rôles et responsabilités des utilisateurs à privilèges sont communiqués de manière informelle.		- Un recensement des utilisateurs à privilège est effectué de manière partielle et peu mis à jour - Une charte administrateur est partiellement documentée pour les utilisateurs à privilèges.		- Les utilisateurs à privilège sont tous connu. Un recensement est réalisé régulièrement ainsi qu'une revue d'accès. - Une charte administrateur est partiellement documentée pour les utilisateurs à privilèges. - Les utilisateurs à privilèges sont entraînés régulièrement afin de comprendre leurs rôles et responsabilités et le risque inhérent à leur statut. - La charte est appliquée, les utilisateurs privilégiés signent la charte informatique ou la charte informatique est annexée au contrat / au règlement intérieur	

Les kits d'exercice de cybercrise de l'ANS

Où trouver les informations ?

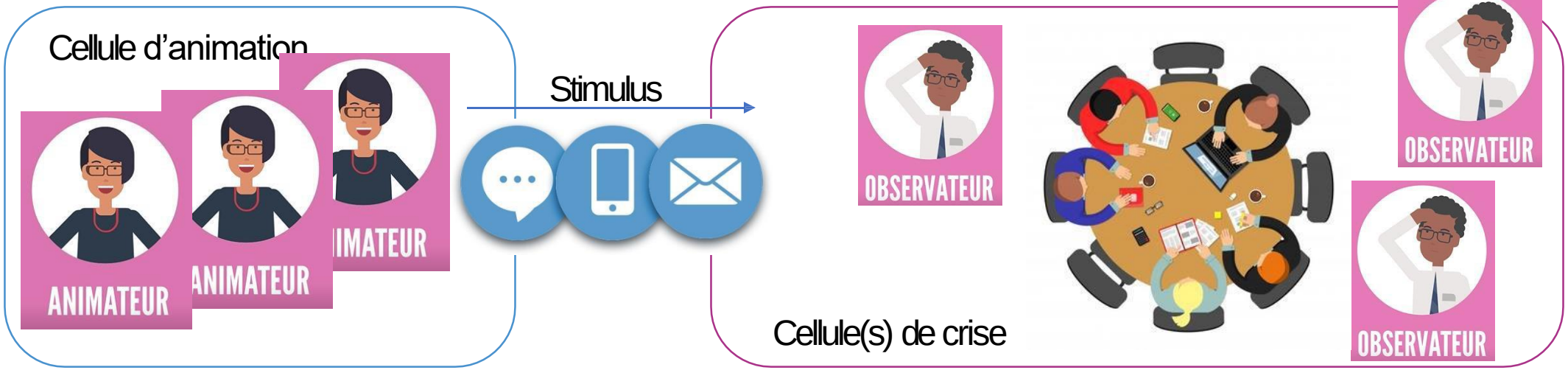
https://www.cyberveille-sante.gouv.fr/

1



Les kits d'exercice de cybercrise de l'ANS

Principes d'organisation



L'animateur met en action le scénario en envoyant les stimuli à la cellule de crise sous forme de simulations d'appels ou de mails pour susciter une réaction / action des joueurs.

Les joueurs s'adaptent à la situation de crise fictive déroulée par l'animateur en utilisant des moyens de communication et procédures opérationnelles habituellement utilisées dans la structure (si elles existent).

L'observateur apporte un regard extérieur à l'exercice et relève les points positifs et axes d'amélioration selon les objectifs de l'exercice. Il n'intervient pas dans le déroulement de l'exercice.

L’exercice

Le Kit ANS Débutant

Avant l'exercice

1. L'animateur s'approprie et adapte à l'ES l'ensemble des documents du kit d'animation avant l'exercice
2. Il s'assure que la structure de santé a transmis les invitations aux joueurs grâce au kit de communication
3. Il récupère la liste des joueurs en faisant compléter l'annuaire des participants à la structure de santé

3 bis. Personnaliser le chronogramme

4. Il envoie le kit participant aux joueurs (ou via la structure de santé) une semaine avant l'exercice

5. Prévoir la logistique

Le Kit ANS Débutant

Pendant l’exercice

1. L'animateur prépare les joueurs à l'exercice en présentant le support de briefing qu'il diffuse dans la salle
2. Il débute l'exercice en lançant par téléphone le premier stimuli présent sur le chronogramme qu'il a imprimé en amont
3. Au cours de l'exercice, il varie le type de stimuli transmis aux joueurs grâce à son livret de stimuli : il pourra en envoyer certains par mail via la boite aux lettres créée pour l'exercice

L'observateur assiste à l'exercice auprès de la cellule de crise et rempli la grille d'évaluation

Financé par l'Union européenne NextGenerationEU

Préparer le Debriefing

Pendant la phase de debriefing, l'observateur participe à la définition des points forts de la cellule de crise et met en avant les axes d'amélioration

4 Une fois l'exercice clos, l'animateur présente le support de debriefing qu'il diffuse dans la salle et distribue le questionnaire de satisfaction pour récupérer les retours des participants

Le Kit ANS Débutant

Après l'exercice

1. L'animateur prend connaissance de la grille d'évaluation remplie par l'observateur ainsi que des retours des joueurs sur le questionnaire

2. Il organise une réunion de restitution d'une heure avec les participants en formalisant un support de présentation à partir des éléments recueillis

3. Selon le mode de fonctionnement choisi, l'animateur pourra transmettre un retour d'expérience anonymisé à l'ARS/GRADeS

Et après ?

Le Kit ANS Débutant

Et après?

- Exemples du Plan d'actions :
  - Réaliser une cartographie des SI / objets connectés / parties prenantes et prioriser les périmètres critiques
  - S'assurer que les sauvegardes sont bien isolées
  - Sensibiliser les interlocuteurs métiers aux termes spécifiques de gestion de crise cyber
  - Préparer des premiers éléments de langage de communication cyber
  - Prévoir un annuaire et une cartographie des personnes, services et bâtiments à notifier en cas de crise
  - Travailler la prise de décision du passage en mode dégradé et les impacts sur les processus métiers, notamment en cas de coupure informatique totale

Créer une instance de suivi du plan d'action
Pour chaque action, définir un responsable et une échéance

Le Kit ANS Débutant

Et après?

- Organiser un exercice de Cyber-crise l'année suivante
  - Utilisation du kit débutant en modifiant le scenario
  - Utilisation du kit intermédiaire
  - Utilisation du guide de l'ANSSI
    https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/

RETEX sur la réalisation d'un exercice : M. Jorge Loureiro, DSIO de l'Hôpital Suisse de Paris

RETEX

Financé par l'Union européenne NextGenerationEU

L'Hôpital Suisse de Paris

Exercice réalisé le 16 juin 2023

Comment être accompagné ?

SESAN

Des prestation d’accompagnement à la réalisation des exercices existent

Accompagnement via le marché régional : ssi@sesan.fr

Accompagnement via les prestataires nationaux

SESAN

Contact

Des questions ?

Contactez : ssi@sesan.fr

Une contribution financière est proposée : AAP IDF

AAP pour la réalisation d'exercices de cyber crise

Objectif	Établissements éligibles	Échéances	Montant financé
Apporter une contribution financière à l'éventuel recours à un prestataire pour réaliser l'exercice	Tous les ES franciliens, par ordre de candidature	AAP ouvert du 18 septembre 2023 au 30 novembre 2023	Forfait de 4 000 euros pour kits niveaux 1 et 2 Forfait de 5 000 euros pour kit niveau 3 (Par exercice et par établissement effectivement mobilisé dans l'exercice. Paiement au service fait)

Pré requis pour candidater

- Renseigner la grille d'autoévaluation
- Mettre à jour l'OPSSIES si cela n'a pas été fait dans les 3 mois précédent la candidature
- Passer commande auprès d'un prestataire

⚠ **Prévoir la présence de la Direction de l'établissement pour l'exercice**

Modalités de candidature

- **Publication de l'AAP sur le site de l'ARS avec le lien vers le formulaire de candidature sur** *démarches simplifiées*
- **Dans ce formulaire l'ES devra renseigner :**
  - Le résultat de son auto-évaluation
  - Le montant de la commande relative à la prestation d'accompagnement
  - La date prévisionnelle de réalisation de l'exercice
  - Le niveau de kit qui sera réalisé
  - La date de dernière mise à jour d'OPSSIES
- **Il devra aussi joindre**
  - La grille d'autoévaluation renseignée
  - Le bon de commande

À terme, il conviendra de joindre la facture afin que l'ARS procède au paiement.

Focus sur les éléments attendus dans l'OPSSIES

Renseignement attendu dans les 3 mois précédant la candidature

Pré requis à la candidature :
→ Il est attendu le renseignement de l'Observatoire Permanent de la Sécurité des Systèmes d'Information des Établissements de Santé (OPSSIES) via OSIS

Exemple de questions à renseigner (non exhaustif)

PGSSI-S	
Avez-vous consulté ou parcouru un document de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-Santé) ?	oui
Avez-vous utilisé un document de la PGSSI-santé?	oui
ORGANISATION	
MP6 - Une personne en charge de la fonction Sécurité du Système d'Information (SSI) ou RSSI est nommée au sein de l'établissement.	oui
La fonction prenant en charge la sécurité des systèmes d'information est elle:	affectée à temps partiel en interne
Le médecin DIM de l'établissement est il impliqué dans la sécurité des données de santé des patients ?	oui
L'établissement est-il doté d'une politique de sécurité ?	oui

En annexes: sont affichées les données à renseigner

Focus sur les audits

Financé par l'Union européenne NextGenerationEU

Réservé pour les Opérateurs de Services Essentiels (OSE)

Lancer la procédure d'inscription sur le site https://club.ssi.rie.gouv.fr

Pour toute information : **club@ssi.gouv.fr**

ANS

Audits Cybersurveillance et Messagerie

Pour tous les ES : https://www.cyberveille-sante.gouv.fr/cybersurveillance

Demander la réalisation d'un audit de cybersurveillance

Pour les GHT, les demandes d'audit se font désormais via une interface de commande d'audit dédiée accessible à l'adresse suivante : https://cybersurveillance.esante.gouv.fr/ . Pour y accéder, il faut disposer d'un compte utilisateur créé par le CERT Santé. La demande de compte doit être adressée à cyberveille@esante.gouv.fr en précisant lenom du GHT, nom/prénom/courriel/ n° de téléphone mobile du RSSI référent. Un guide d'utilisation de cette nouvelle interface est disponible ici .

Pour les autres établissements, les demandes d'audit doivent être adressées à cyberveille@esante.gouv.fr et les différents échanges se feront en direct avec les responsables du service. Le message de demande doit préciser le nom des domaines exposés et le nom/prénom/courriel/ n° de téléphone mobile du responsable de l'audit.

Pour encadrer la réalisation de l'audit par l'ANS, une convention est mise en place. Elle précise le périmètre de l'audit, le calendrier de réalisation et les points de contact pour faciliter les échanges.

Le rapport est communiqué dans un délai de quinze jours à la suite des travaux. Si toutefois des vulnérabilités critiques étaient identifiées au cours de l'audit, celles-ci seront notifiées avant l'envoi du rapport.

Rappel : les bonnes pratiques

Bonnes pratiques

Synthèse des ressources disponibles

- Kit de sensibilisation "Tous Cybervigilants" :https://esante.gouv.fr/sites/default/files/2022-01/kit-com-cybersecurite-etablissements-sante.zip
- Kit de sensibilisation CyberMalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation

https://www.cybermalveillance.gouv.fr/bonnes-pratiques

- CyberveilleSanté : https://cyberveille-sante.gouv.fr/
- Newsletter SESAN : https://segurnumerique.sante-idf.fr/animation-regionale/cybersecurite/
- Autres liens utiles :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales
https://www.ssi.gouv.fr/particulier/precautions-elementaires/dix-regles-de-base/
https://www.ssi.gouv.fr/particulier/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/

Offre SESAN

SESAN

Offres d'accompagnement

Missions du Département SSI:

- Renforcement de la cybersécurité des ES et ESMS franciliens
- Animation de la communauté RSSI Santé régionale
- Mutualisation de solutions régionales

SESAN

Offres d'accompagnement

Financé par l'Union européenne NextGenerationEU

Cabinet de ville / CPTS

Exercice libéral

en cabinet de ville

CYBER SERVICES MUTUALISES

S'informer et s'équiper contre tous types de cybermenaces !

- Webinaires thématiques
- Supports de sensibilisation
- Sensibilisation à la cybersécurité
- Test de phishing

SESAN

Offres d'accompagnement

Petites et moyennes structures (Médico-Social – MSP – DAC…)

Petites et moyennes structures

Médico-Soc - MSP - DAC...

CYBER SERVICES MUTUALISES

Le b.a.-ba - S'informer c'est déjà se protéger

- Webinaires thématiques
- Supports de sensibilisation
- Plateforme d'échange
- Base documentaire
- Dossier de conformité
- Alertes ANSSI et ANS

CYBER SERVICES PRÉVENTION

Se prémunir contre tous types de cybermenaces dans votre établissement

- Sensibilisation à la cybersécurité
- Test de phishing
- Escape Game
- Audit de sécurité
- Exercice de cybercrise

CYBER SERVICES PROTECTION

Du diagnostic à la (ré)action

- Cybersurveillance
- Scan de vulnérabilité
- Transferts sécurisés
- Plan de continuité
- Assistance gestion de crise

Financé par l'Union européenne NextGenerationEU

SESAN

Offres d'accompagnement

Financé par l'Union européenne NextGenerationEU

Etablissements Sanitaires et grandes structures Médico-Sociales

Etablissements sanitaires
et grandes structures Médico-Social

CYBER SERVICES MUTUALISES

Le b.a.-ba - S'informer c'est déjà se protéger

- Webinaires thématiques
- Supports de sensibilisation
- Plateforme d'échange
- Base documentaire
- Dossier de conformité
- Alertes ANSSI et ANS

CYBER SERVICES PRÉVENTION

Se prémunir contre tous types de cybermenaces dans votre établissement

- Sensibilisation à la cybersécurité
- Test de phishing
- Escape Game
- Audit de sécurité
- Exercice de cybercrise
- Cartographie
- Analyse de risque en SaaS

CYBER SERVICES PROTECTION

Du diagnostic à la (ré)action

- Cybersurveillance
- Scan de vulnérabilité
- Transferts sécurisés
- Plan de continuité
- Assistance gestion de crise

SESAN

Offres d'accompagnement

https://cyberservices.sante-idf.fr

Pour toute information : ssi@sesan.fr

Annexes

Annexes

Renseignement de l'OPSSIES (1/3)

SÉCURITÉ SI

ADRESSE FONCTIONELLE SSI

Adresse courriel SSI

PART DU NUMERIQUE

AUDIT DE CYBERSURVEILLANCE (ANS)

	Audit récent	Audit précédent
Date audit de cybersurveillance		
Nombre de domaines		
Appréciation		
Total vulnérabilités		
Nombre de vulnérabilités critiques		
Nombre de vulnérabilités hautes		
Nombre de vulnérabilités moyennes		
Nombre de vulnérabilités faibles		

AUDIT DE CYBERSURVEILLANCE (ANS) - GHT

	Audit récent	Audit précédent
Date audit de cybersurveillance		
Nombre de domaines		
Appréciation		
Total vulnérabilités		
Nombre de vulnérabilités critiques		
Nombre de vulnérabilités hautes		
Nombre de vulnérabilités moyennes		
Nombre de vulnérabilités faibles		

Renseigné par l'ANS

AUDIT ADS - ACTIVE DIRECTORY (ANSSI)

	Audit récent	Audit précédent
Date audit Active Directory		
Niveau ADS		
Score ADS		
Nombre d'audits ADS		
Nombre d'utilisateurs		

AUDIT ADS - ACTIVE DIRECTORY (ANSSI) - GHT

	Audit récent	Audit précédent
Date audit Active Directory		
Niveau ADS		
Score ADS		
Nombre d'audits ADS		
Nombre d'utilisateurs		

Renseigné par l'ANSSI

Financé par l'Union européenne NextGenerationEU

Annexes

Renseignement de l'OPSSIES (2/3)

AUDIT ADS - ACTIVE DIRECTORY (ANSSI) - GHT		
	Audit récent	**Audit précédent**
Date audit Active Directory		
Niveau ADS		
Score ADS		
Nombre d'audits ADS		
Nombre d'utilisateurs		

Renseigné par l'ANSSI

PGSSI-S	
Avez-vous consulté ou parcouru un document de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-Santé) ?	oui
Avez-vous utilisé un document de la PGSSI-santé?	oui
ORGANISATION	
MP6 - Une personne en charge de la fonction Sécurité du Système d'Information (SSI) ou RSSI est nommée au sein de l'établissement.	oui
La fonction prenant en charge la sécurité des systèmes d'information est elle:	affectée à temps partiel en interne
Le médecin DIM de l'établissement est il impliqué dans la sécurité des données de santé des patients ?	oui
L'établissement est-il doté d'une politique de sécurité ?	oui
CONNAISSANCE DES RISQUES	
MP1 - L'établissement dispose d'une cartographie des risques liés aux services numériques actualisée annuellement basée sur une méthodologie qui permette de comparer les résultats d'une itération à l'autre.	oui datant de moins d'1 an
MP2 - La cartographie des risques liés aux services numériques est consolidée dans une cartographie globale des risques portant sur l'établissement.	oui
MP3 - Une analyse de risque, validée par les responsables métiers des services concernés, est réalisée lors de l'introduction d'un nouveau service numérique (application, matériel IT, équipement biomédical et technique, GTB/GTC) .	oui, systématiquement
BUDGET SECURITE NUMERIQUE	
SECURISATION - MISE EN CONFORMITE	
INDICATEURS ET TABLEAU DE BORD	
Un indicateur périodique permet il de mesurer le nombre d'incidents survenus?	non
Quel est le nombre d'indicateurs périodiques relatifs à la sécurité de l'information?	6 à 20
CONTEXTE	
La connexion de terminaux personnels (smartphone, tablette) est-elle autorisée sur le SIH (BYOD) ?	oui
MP11a - Un inventaire des matériels (Matériel: postes de travail, serveurs, machines virtuelles, équipements réseau, biomédical, etc) est réalisé et publié annuellement	oui, datant de moins d'1 an
MP11b - Un inventaire des logiciels (postes de travail, serveurs, machines virtuelles, équipements réseau, biomédical, etc) est réalisé et publié annuellement	oui, datant de moins d'1 an
MP12 - Une cartographie applicative est réalisée et tenue à jour (flux d'échange entre applications et ensemble des flux) sur la base de celles demandées par l'ANSSI (Cartographie du Systèmes d'Information).	oui, datant de moins d'1 an
MP20a - L'établissement met en œuvre des réseaux cloisonnés pour le WIFI patient	oui
MP20b - L'établissement met en œuvre des réseaux cloisonnés pour le WIFI SI ES	oui

Renseigné par l'établissement

Financé par l'Union européenne NextGenerationEU

Annexes

Renseignement de l'OPSSIES (3/3)

Existe-t-il des accès à distance sur le SIH accessibles par le personnel médical de l'établissement?	non
Existe-t-il des accès à distance sur le SIH accessibles par les professionnels de santé libéraux?	non
Existe-t-il des accès à distance sur le SIH accessibles par les patients de l'établissement?	non
Existe-t-il des accès à distance sur le SIH pour les opérations de télémaintenance ou téléassistance des industriels ?	oui
MESURES	
Pour quelle proportion des professionnels de santé, la carte CPx (CPS,CPE) est-elle utilisée pour contrôler l'accès aux données de santé personnelles contenues dans le SIH ?	0-25%
La carte CPx (CPS,CPE) est-elle utilisée pour contrôler l'accès physique aux bâtiments?	non
La carte CPx (CPS,CPE) est-elle utilisée pour d'autres usages (cantine, photocopieuse, autres) ?	non
La carte CPx (CPS, CPE) est-elle utilisée en mode sans contact ?	non
Une revue des comptes d'accès au SIH est elle réalisée périodiquement ?	oui, moins d'une fois par an
Une revue des droits d'accès au SIH est elle réalisée périodiquement ?	oui, moins d'une fois par an
Une revue des comptes d'accès aux applications de soins est elle réalisée périodiquement ?	oui, moins d'une fois par an
Une revue des droits d'accès aux applications de soins est elle réalisée périodiquement ?	oui, moins d'une fois par an
Pour chaque professionnel de santé de l'établissement, l'identifiant RPPS ou ADELI est-il renseigné et à jour dans le SIH?	oui, totalement
Les équipements bio médicaux connectés au réseau sont- ils inclus dans le périmètre SSI ?	oui
Existe-t-il un suivi des déclarations et demandes d'autorisation CNIL?	oui, au moins une fois par an
Les matériels qui sont réaffectés au sein du SI ou qui sortent du SI (vente, recyclage, mise au rebus) font-ils l'objet de dispositions spécifiques pour assurer la confidentialité des données qu'ils stockaient ?	oui
MP28 - Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques sont réalisées	oui, au moins une fois par jour
MP31 - Des tests de restauration a minima sur échantillons représentatifs sont réalisés.	oui, périodiquement
Existe-t-il un traçage des actions uilisateurs (accès, lecture, écriture, etc.) sur le SIH?	oui, en partie
Les traces des actions utilisateurs peuvent-elles être lues et comprises par quelqu'un d'autre qu'un informaticien ?	oui, en partie
CONTRÔLE ET AUDIT	
MP17 - L'organisation de la sécurité du système d'information fait l'objet, tous les trois ans, d'un audit organisationnel de la SSI dans l'esprit de l'ISO 27001	oui, plus d'1 fois par an
En cas d'audit régulier réalisé en dehors de l'esprit de la norme ISO 27001, quel est le référentiel d'audit d'organisation utilisé ?	PSSI établissement
Quand a été effectué le dernier audit SSI ?	Non renseigné
REACTION AUX INCIDENTS	
MP39 - L'établissement a défini et applique une procédure interne de remontée des incidents de sécurité SI qui associe les métiers concernés	oui, totalement
IDENTIFICATION ELECTRONIQUE	

Renseigné par l'établissement

Financé par l'Union européenne NextGenerationEU