

SANTÉ NOU SÉ FOS NOU

Dire oui à la e-Santé ? C'est le moment ou jamais !



PARLONS CYBERSÉCURITÉ

Le Cybermoi/s, c'est le moment incontournable pour adopter toutes les bonnes pratiques et protéger votre vie numérique avec tous les acteurs engagés. Et ça commence maintenant !

La gestion des dossiers patients informatisés, des dispositifs médicaux, des prescriptions et plus récemment l'arrivée de Mon Espace Santé, qui permet de stocker, partager des documents avec les équipes de soin, posent inévitablement la question de la confidentialité, d'une part... Mais aussi celle de la sécurité des données de santé. La dernière attaque en date, celle de l'Hôpital de Corbeille Essonne, montre à quel point les menaces et les attaques fragilisent notre système de santé. La Cybersécurité devient donc un enjeu majeur pour tous les acteurs de la société.

Attaque extérieure ou erreur « intérieure », la résilience du système reposera en grande partie sur sa capacité à limiter la casse en cas de cyberattaque, en s'équipant de solutions numériques sécurisées avec des protocoles bien balisés, des authentifications fortes...

Ainsi, au même titre que la société qui, après l'émergence de la voiture, s'est organisée et en prenant des mesures pour rendre ce mode de transport plus sécurisant, le développement des Internet a conduit progressivement à :

- La mise en place d'infrastructures (serveurs, câbles sous-marins, fibres...)
- La définition de règles et codes (RGPD) permettant d'accompagner ce développement

Au-delà de la vision d'ensemble, c'est une culture commune qu'il nous faut collégialement développer pour que tout un chacun prenne conscience de son impact sur le système d'information, et des précautions à prendre à titre individuel pour améliorer la sécurité en ligne et aider à se prémunir contre les actes de cybermalveillance.

DANS LE PRÉSENT NUMÉRO :

Stratégie régionale
Cybersécurité - 2
Conseils de la CNIL - 3
Chiffres clés & calendrier - 4



**Ensemble,
soyons tous cybervigilants.**

STRATÉGIE RÉGIONALE CYBERSÉCURITÉ

Une priorité pour réussir la transformation numérique

Les agences régionales de santé (ARS) s'assurent de la déclinaison territoriale de la politique de sécurité numérique en santé.

L'ARS Martinique renforce l'animation territoriale et accompagne le volet Cyber du virage numérique : sensibilisation des acteurs, partage de pratiques, recherche de mutualisations, organisation de la réponse à un incident au niveau du territoire de santé, contrôle du niveau de maturité Cyber et des plans d'actions continus des structures de santé.

4 ambitions

- Inscrire la cybersécurité au cœur du dispositif de gouvernance des établissements de santé afin que ce sujet soit porté à un niveau stratégique
- Constituer une taskforce cyber régionale pour renforcer et tirer parti de la force du collectif (partage de bonnes pratiques, développement de la coopération et de l'esprit d'entraide) et la mutualisation (prestations, ressources RH & techniques, etc.)
- Instaurer une véritable hygiène numérique au sein des établissements de santé (organisation, utilisateurs, patients usagers) : déclaration des incidents & protection des outils de travail
- Renforcer la sécurité numérique (audits Cyber, plan de remédiation des vulnérabilités, information et sensibilisation acteurs, etc.)

“

*l'ARS avec l'appui
du GRADeS
Martinique,
accompagne
significativement les
établissements de
santé dans le but
d'élever le niveau de
maturité de leur
Système
d'Information.*

QUELLES SONT LES PRINCIPALES VULNÉRABILITÉS D'UNE STRUCTURE DE SANTÉ ?



LOGICIELS/SYSTÈMES NON CORRIGÉS
OU OBSOЛÈTES



MANQUE DE VISIBILITÉ ET D'INVENTAIRE
DES SYSTÈMES NUMÉRIQUES



CONTRÔLES INSUFFISANTS
DE LA CYBERSÉCURITÉ DES SYSTÈMES
PÉRIPHÉRIQUES



GRANDE VARIÉTÉ DE PROTOCOLES,
DE FOURNISSEURS ET DE PÉRIPHÉRIQUES
MANQUE D'OPÉRABILITÉ



COMPOSANT CRITIQUE DU SI
INSUFFISAMMENT SÉCURISÉ
(SAUVEGARDE, ACTIVE DIRECTORY)



COMPLEXITÉ DUE À
DES RESPONSABILITÉS DIFFUSES
DSI - BIOMÉDICAL - MOYENS GÉNÉRAUX...

PORTAIL DE VEILLE, D'ALERTE & D'ÉCHANGE

www.cyberveille-sante.gouv.fr

LE CERT SANTÉ

cyberveille@esante.gouv.fr

+33 972 43 91 25

9h-18h du lundi au vendredi

HFDS/FSSI

ssi@sg.social.gouv.fr

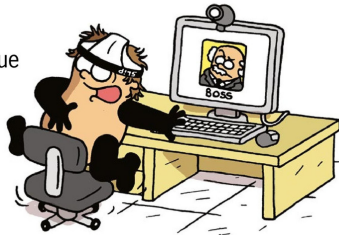
L'ANSSI

cert-fr.cossi@ssi.gouv.fr

10 conseils de la CNIL pour rester Net sur le Web

1 Réfléchir avant de publier

Sur internet, tout le monde peut voir ce que tu publies : photos, vidéos, opinions, etc.



2 Respecter les autres

Tu es responsable de ce que tu publies sur les réseaux sociaux... Ne fais pas aux autres ce que tu ne voudrais pas que l'on te fasse.



3 Ne pas tout dire

Donner le minimum d'informations sur soi en ligne, c'est se protéger ! Mieux vaut ne pas communiquer tes opinions, ta religion ou ton numéro de téléphone...



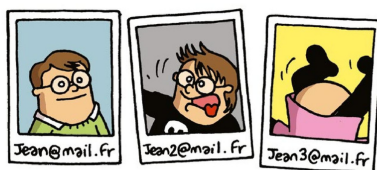
4 Sécuriser ses comptes

En paramétrant tes profils sur les réseaux sociaux, tu restes maître des informations que tu souhaites partager.



5 Créer plusieurs adresses mail

Tu peux par exemple utiliser une adresse pour les jeux vidéos, une pour tes amis et une autre boîte e-mail pour les réseaux sociaux.



6 Faire attention à tes photos et tes vidéos

Envoyer, publier une photo ou une vidéo gênante de soi ou des autres, c'est risquer une diffusion incontrôlable.



7 Utiliser un pseudonyme

Seules les personnes à qui tu l'auras communiqué sauront qu'il s'agit de toi et suivront tes aventures sur le net.



8 Protéger ses mots de passe

Il faut qu'il soit difficile à deviner et différent pour chaque service. Évite d'utiliser ton surnom ou bien ta date de naissance par exemple. Et surtout, garde-le pour toi !



9 Nettoyer ses historiques

Pour éviter d'être tracé, il est conseillé d'effacer régulièrement tes historiques de navigation et d'utiliser la navigation privée si tu utilises un ordinateur ou un smartphone qui n'est pas le tien.



10 Surveiller sa réputation en ligne

Taper ton nom dans un moteur de recherche te permet de savoir ce qui est dit sur toi sur internet et quelles informations circulent.



Partage ces conseils
avec tes amis et ta famille
pour qu'ils protègent eux aussi leur vie privée !

CNIL
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Retrouvez d'autres conseils sur www.cnil.fr

SÉCUR NUMÉRIQUE

Chiffres clés mi-2022

39%

d'établissements sociaux & médico-sociaux ont **candidaté** à l'appel à projet ESMS numérique

100%

des groupements de laboratoires sont **en cours d'acquisition d'une solution Ségur compatible & d'une messagerie sécurisée de santé**

83%

des établissements sanitaires ont un **logiciel Ségur commandé**



MÉDICO-
SOCIAL



MÉDECINE
DE VILLE



OFFICINE



BIOLOGIE
MÉDICALE



RADIOLOGIE



HÔPITAL

CALENDRIER

Appel à projets & financements



Financé par
l'Union européenne
NextGenerationEU

Octobre

ESMS NUMÉRIQUE
Résultat de l'AAP #3 2022

Publication de l'appel à projets #4 à venir sur le site de l'ARS Martinique.



30/10

SUN-ES
Clôture de la fenêtre 3

Tous les établissements sanitaires quel que soit leur statut juridique et leur type d'activité sont concernés.



30/11

SONS
Limite des commandes

Commandes de logiciel Ségur compatible pour les RIS ; SGL, LOINC ; LGC ; RI, DPI, PFI.



18/12

SONS
Limite des commandes

Commandes de logiciel Ségur compatible pour les LGO.



GLOSSAIRE

Cyber

Préfixe généralement utilisé pour signifier une dimension informatique et réseau à la notion qu'il accompagne (Cyber-harcèlement, Cyberguerre...). Le terme vient du grec Kubernêtikê, signifiant « gouvernail ».

RGPD

Règlement Général sur la Protection des Données. Nom français du « General Data Protection Regulation ».

SSI

La sécurité des systèmes d'information, plus communément appelée INFOSEC, fait référence aux processus et méthodologies impliqués pour garder les informations confidentielles, disponibles et assurer leur intégrité.

Cybersécurité

Protection des systèmes connectés à Internet, comprenant le matériel, les logiciels et les infrastructures associées, les données et les services qu'ils fournissent, contre tout accès non autorisé, tout dommage ou tout usage abusif.

Hacker

« Fouineur » ou « White Hat », personne qui par jeu, goût du défi ou soucis de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique. À ne pas confondre avec le cybercriminel ou « Black Hat », dont l'intention est clairement de nuire.