MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

EXAMEN PROFESSIONNEL DE TECHNICIEN DE CLASSE SUPERIEURE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2023 -

Mercredi 13 avril 2022

SUJET : RESEAUX DE TELECOMMUNICATIONS ET EQUIPEMENTS ASSOCIES

Epreuve écrite unique d'admission consistant à partir d'un dossier à caractère technique, en une étude de cas faisant appel à des connaissances relatives à l'environnement et à la technique des systèmes d'information et de communication et permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

(Durée : 3 heures – Coefficient 1)

Le dossier documentaire comporte 23 pages. (hors page d'énoncé du sujet).

Il vous est rappelé que votre identité ne doit figurer que dans l'en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettez en fin d'épreuve entrainera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A …, B…, Y…, Z…).

IMPORTANT

1. LES COPIES SERONT RENDUES EN L'ÉTAT AU SERVICE ORGANISATEUR. A L'ISSUE DE L'ÉPREUVE, CELUI-CI PROCÉDERA À L'ANONYMISATION DE LA COPIE.
2. NE PAS UTILISER DE CORRECTEUR D'ORTHOGRAPHE SUR LES COPIES.
3. ECRIRE EN NOIR OU EN BLEU – PAS D'AUTRE COULEUR.
4. IL EST RAPPELÉ AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE SUR LA COPIE.

SUJET

Vous êtes affecté en tant que technicien SIC de classe supérieure dans le service informatique d'un commissariat de police, récemment installé dans un nouveau batiment.

Afin de faciliter le nomadisme numérique de l'ensemble des personnels, votre chef de service vous demande une note technique sur l'étude de la mise en place de réseaux wifi dans ce batiment afin de répondre aux différents usages suivants :
l'accès sans fil sur le réseau interministériel (RIE) ;
l'accès sans fil à un réseau internet grand public (utilisation outils de visio conférence, accès invités pour matériels personnels) ;
l'accès sans fil à un réseau internet spécialisé (enquêteurs de police spécialisés aux métiers judiciaires).

En vous appuyant sur vos connaissances et les documents annexes,vous rédigerez une étude technique, non nominative et non signée, présentant les éléments suivants :

Question 1
Un rappel général sur ce que représente un réseau sans fil wifi.
Vous décrirez également ses avantages, inconvénients et les risques qu'il introduit (besoins de traçabilité, risques juridiques).
Selon vous, de quelles informations sont consituées les "données de trafic" ?

Question 2
La conception et la description du schéma d'architecture réseau représentant la solution que vous préconiseriez dans le cadre du besoin exprimé par votre responsable.
Vous veillerez à mentionner les prérequis techniques nécessaires, les catégories d'équipements utilisés et les différents flux.
Vous compléterez ce schéma d'une proposition de bon de commande (non chiffré) à présenter à votre chef de service pour la solution retenue. Vous justifierez vos choix de matériels, la quantité choisie pour chaque équipement listé, ainsi que le mode opératoire à suivre pour faire ces achats.

Question 3
La description des différentes étapes du plan de déploiement (planning, organisation, ...) afin de mettre en oeuvre la solution choisie.
Il conviendra également de préciser :
- les moyens utilisés ;
- la manière dont le support sera mis en place autour de cette solution ;
- la documentation utile à cette nouvelle offre de service.

Dans le cadre des tests de bon fonctionnement, quelles commandes exécuteriez vous pour vérifier
- la configuration ip ?
- La connectivité d'un équipement sur le réseau ?
Connaissez-vous l'unité de mesure de l'intensité du signal wifi ?

Dossier documentaire :

DOCUMENT 1

Source : https://www.murielle-cahen.com/publications/p_wi-fi.asp

I. Le cadre réglementaire actuel d'exploitation des réseaux Wi-Fi

L'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) a rappelé, dans le cadre de sa décision du 23 mai 2001, les usages possibles des technologies de type Wi-Fi. Elle distingue selon que le réseau est destiné à une utilisation à l'intérieur ou à l'extérieur de bâtiments.

A. Utilisation à l'intérieur des bâtiments

Les entreprises, les collectivités territoriales ou les particuliers peuvent utiliser la technologie wi-fi pour installer un réseau à l'intérieur de leurs immeubles sous réserve des conditions de respecter les valeurs maximales de puissance rayonnée.

La puissance maximale autorisée à l'intérieur des bâtiments est de 10mW pour l'ensemble de la bande 2,4 GHz (2400 MHz et 2483,5 MHz) et de 100mW pour les fréquences comprises entre 2446,5 MHz et 2483,5 MHz.

L'utilisation des fréquences 5150 MHz - 5350 MHz est autorisée à l'intérieur des bâtiments avec une puissance maximale de 200mW.

Le 9 février 2015, la loi n° 2015-136 dite loi abeille relative à la sobriété, à la transparence, à l'information et à la concertation en matière d'exposition aux ondes électromagnétiques est entrée en vigueur.

Elle renforce le rôle des maires à ce sujet. L'article 1 de la loi prévoit ainsi que « toute personne qui exploite sur le territoire d'une commune une ou plusieurs installations radioélectriques (…) transmet au maire ou au président de l'intercommunalité, à sa demande un dossier établissant l'état des lieux de ces installations. » L'implantation et la modification substantielle d'un site émettant des ondes électromagnétiques doivent également faire l'objet d'un rapport transmis au maire. Avant l'implantation d'une installation, le maire peut exiger une simulation de l'exposition aux ondes émises par celle-ci.

Cette loi prévoit aussi que les établissements proposant au public un accès wifi doivent le mentionner clairement à l'aide d'un pictogramme visible à l'entrée du bâtiment (article 4). Pour les établissements accueillant des enfants de moins de 3 ans, la loi interdit l'utilisation du wifi dans les espaces réservés à l'accueil, au repos et aux activités (article 7). Pour les classes des écoles primaires, le wifi doit être coupé s'il n'est pas utilisé pour les activités pédagogiques.

B. Utilisation à l'extérieur des bâtiments

La puissance maximale autorisée à l'extérieur des bâtiments est de 100mW, sur les propriétés privées ou sur le domaine privé des personnes publiques, pour les seules fréquences comprises entre 2446,5 Mhz - 2483,5 MHz. Cette utilisation reste soumise à une procédure d'autorisation préalable avec avis du Ministère de la défense.

L'utilisation à l'extérieur des bâtiments sur le domaine public n'est pas autorisée.

Pour résumer, les RLAN à l'extérieur des bâtiments et sur le domaine public sont interdits ; ils sont en revanche autorisés à l'intérieur des bâtiments et à l'extérieur tant qu'il s'agit d'un domaine privé et tant que les émetteurs respectent des limites de puissance.

II. Les nouvelles règles adoptées pour l'expérimentation des réseaux locaux radio-électriques (RLAN) ouverts au public

L'Autorité de Régulation des Télécommunications a adopté le 7 novembre 2002 les décisions permettant, à compter de janvier 2003 et dans 38 départements pilotes, l'utilisation de réseaux Wi-Fi pour la fourniture au public de services Internet haut débit, en particulier dans les lieux de fort passage du public (dits "hot spots") comme les gares, les aéroports, les centres d'affaires ou encore les hôtels. Au jour d'aujourd'hui le nombre de départements où l'exploitation de réseaux Wi-Fi est autorisée est 58.

Le même jour, l'ART (à l'époque) avait arrêté les lignes directrices fixant les conditions d'expérimentation de réseaux RLAN ouverts au public, sur la bande de fréquence des 2,4 GHz.

Ces expérimentations ne pourront être conduites qu'après la délivrance d'une autorisation, qui sera délivrée gratuitement, sur la base de l'article L.33-1 du code des postes et télécommunications pour une durée maximale de dix-huit mois.

III. Les enjeux juridiques du Wi-Fi

Le non-respect de l'ensemble de ces dispositions fait l'objet de sanctions prévues par le Code des Postes et des Télécommunications.

Ainsi, le fait d'établir ou de faire établir un réseau indépendant (de type Wi-Fi) sans autorisation ou le fait de le maintenir en violation d'une décision de suspension ou de retrait de cette autorisation est puni d'un emprisonnement de six mois et d'une amende de 30.000 euros (article L.39-1 alinéa 1 CPT).

Sont donc visés, aussi bien les installateurs que les entreprises qui ont souhaité l'installation de tels réseaux.

Il est également interdit de perturber, en utilisant une fréquence, un équipement ou une installation radioélectrique, dans des conditions non conformes aux dispositions de l'article L. 34-9 ou sans posséder l'autorisation prévue à l'article L. 89 ou en dehors des conditions réglementaires générales prévues à l'article L. 33-3, les émissions hertziennes d'un service autorisé (article L.39-1 alinéa 2 CPT).

L'utilisation du réseau Wi-Fi peut, par ailleurs, poser des problèmes tant techniques que juridiques, quant, notamment, à son niveau de sécurisation. En effet, un des inconvénients de la technologie Wi-Fi est la possibilité "d'écouter" les transmissions de données, notamment du fait d'une faille de sécurité dans la phase d'autorisation d'accès au réseau sans fil.

Bien que des nouveaux outils de sécurisation sont déjà en voie d'élaboration (par exemple remplacement du protocole à clé fixe appelé WEP par un nouveau système de chiffrement), des nouveaux types de piratage informatique sont susceptibles d'apparaître.

Le RGPD (règlement général sur la protection des données) met en place de nouveaux droits pour les personnes physiques dont les données sont collectées. Il impose également de nouvelles obligations pour ceux qui traitent ces données. Le RPGD est un règlement européen qui encadre la protection des données personnelles. Il a été adopté par le parlement européen en avril 2016 et est entré en vigueur le 25 mai 2018.

Il renforce le principe du consentement de la personne pour l'utilisation de ses données. Le consentement explicite est devenu grâce à ce texte une obligation. L'accord doit donc être clair et sans ambiguïté. Ceux qui collectent ces données doivent informer les personnes sur ce qu'elles vont devenir, le but de cette collecte. Si un incident survient ne permettant plus la protection de ces données il faut que les personnes qui ont consenti à leur collecte en soient informées. Les autorités doivent également être alertées dans cette situation.

Ces données doivent pouvoir être transmises, modifiées et effacées à la demande des propriétaires. Les données sensibles telles que les données médicales doivent bénéficier du plus haut niveau de sécurité. Pour les entreprises de plus de 250 salariés, un registre doit être établi sur la conformité du traitement des données avec le RGPD.

Les entreprises qui traitent ces données doivent avoir une raison légitime pour le faire. Elles doivent utiliser aussi peu de données que nécessaires. Cela peut être problématique pour les établissements proposant un accès gratuit au wifi comme les gares, cafés, bibliothèques ou les magasins. Ils ont pour habitude de proposer un accès libre au wifi, mais pour ce faire ils vendent les données collectées des internautes qui utilisent leur réseau à des entreprises. La mise en place d'un réseau wifi dans ces infrastructures a en effet un coût qu'il faut nécessairement compenser.

DOCUMENT 2

Source : https://www.alliance-informatique.fr/revue-blog/comment-vous-assurez-de-la-conformite-reglementaire-de-vos-reseaux-wifi/

Comment assurer la conformité réglementaire de vos réseaux WiFi ?

Donner accès à Internet est soumis à des obligations strictement encadrées par la loi.

Pour répondre aux usages mobiles, les entreprises ont déployé des réseaux sans fils (dans l'espace de travail, à la cafeteria ou à la terrasse d'un café par exemple) en parallèle de leurs réseaux filaires.
En matière de services, le réseau WiFi de l'entreprise peut remplir plusieurs objectifs : accès qualitatif des terminaux mobiles au SI, stratégie BYOD, accès internet pour les visiteurs professionnels, internet gratuit pour les clients, etc.
Ce trafic, en net augmentation, complexifie fortement la gestion du réseau au niveau de la sécurité.

La sécurité des réseaux WiFi est mise en cause

Par le passé, les mises en garde étaient essentiellement destinées contre les dangers des hotspots publics, **aujourd'hui les réseaux WiFi Privés sont aussi concernés.**
En octobre 2017, un chercheur a découvert une importante vulnérabilité, au sein du protocole WPA2 de sécurisation des connexions WiFi. Cette faille, baptisée krack, entraîne un risque d'interception de données, de détournement de l'utilisateur vers des sites et services malveillants, ou encore d'injection de données à son insu.
Le cheval de Troie Switcher cible Android pour attaquer les réseaux WiFi. Il ne s'attaque pas directement aux utilisateurs mais fait d'eux des complices involontaires en déplaçant physiquement les sources de l'infection.
Vous aimez aussi ce bar-café parce qu'il vous offre un accès WiFi gratuit … votre voisin(e) a démarré un des nombreux logiciels gratuits de sniffing, et dans un premier temps a capté les adresses URL des pages visitées par les clients du café, et ensuite des informations beaucoup plus privées (Identifiants de comptes mail, Adresses mail, Mots de passe, etc.).
Mais cela va encore plus loin… on peut renifler à la volée les cookies informatiques des voisins de table. Ces cookies, stockent des identifiants (ex : Facebook, Twitter, Yahoo Mail, Amazon, Flickr, Google, etc.), qui peuvent être ensuite utilisés pour se connecter à votre insu.

Suivez-vous la réglementation wifi en entreprise ?

Le respect de la réglementation en la matière oblige les entreprises à apporter un traitement différent selon la destination des réseaux WiFi.
La mise en place d'un réseau WiFi ouvert au public et ses incidences en matière de traitement de données à caractère personnel est soumise à l'article L34-1 du Code des postes et des communications électroniques.
La loi n° 2006-64 du 23 janvier 2006, relative à la lutte contre le terrorisme, a étendu cette obligation à l'ensemble des personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit.
Le décret du 24 mars 2006 a ainsi créé un nouvel article R.10-13 du CPCE, qui décrit les catégories de données à conserver. Il s'agit :

- des informations permettant d'identifier l'utilisateur (par exemple : adresse IP, numéro de téléphone, adresse de courrier électronique) ;
- des données relatives aux équipements terminaux de communication utilisés ;
- des caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
- des données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- des données permettant d'identifier le ou les destinataires de la communication.
- Pour les activités de téléphonie : les données permettant d'identifier l'origine et la localisation de la communication.

Le décret du 24 mars 2006 fixe la durée de conservation des données à un an, durée au-delà de laquelle elles devront être anonymisées. Ce délai de conservation court dès l'enregistrement des données.
La nouvelle règlementation RGPD ne comporte pas de nouveautés concernant le traitement des données dans le cadre de la fourniture au public de services de communication électronique. S'applique alors les dispositions de la loi Informatiques et Libertés, notamment l'information des utilisateurs de la présence d'un tel traitement.

La CNIL, dans l'immédiat, considère que les entreprises et les administrations fournissant un accès internet à leurs employés ne sont pas concernées par cette obligation de conservation.
Au-delà, un employeur a le droit de mettre en œuvre un dispositif de surveillance de l'activité de ses salariés (contrôle de la messagerie, des sites internet consultés, etc.) dès lors qu'un certain nombre de garanties sont respectées, en particulier, l'information des intéressés sur le système mis en œuvre et la déclaration préalable du dispositif auprès de la CNIL.

Des sanctions importantes

Tout manquement à l'obligation de conservation des données expose la personne à laquelle incombe cette obligation aux sanctions visées à l'article L. 39-3 du CPCE, **soit un an d'emprisonnement et 75.000 euros d'amende pour les personnes physiques, et 375.000 euros pour les personnes morales** (en application de l'article 131-38 du code pénal).

L'occasion d'adopter de bonnes pratiques

Certains fournisseurs proposent des solutions de bout en bout qui englobent l'ensemble des réseaux filaires et sans fil de l'entreprise. Dans l'immédiat, il est préférable, de reconnaître les limites (en matière de contrôle) des outils existants.
Dans ce contexte de vulnérabilité et de réglementation, nous vous conseillons fortement :

- A titre privé, d'utiliser des accès WiFi sécurisés de type portail captif, et de recourir à des services VPN, au moins lors de l'utilisation de hotspots

- Au sein de l'entreprise, de mettre en place un portail captif WiFi, avec de nouvelles pratiques d'isolation des réseaux et des terminaux connectés à un même point d'accès.

Les règles de sécurité | Agence nationale de la sécurité des systèmes d'information

Source : https://www.ssi.gouv.fr/entreprise/protection-des-oiv/les-regles-de-securite/

Les règles de sécurité sont à la fois organisationnelles et techniques. Elles doivent, pour la plupart, être déjà appliquées par l'ensemble des opérateurs pour sécuriser efficacement leurs systèmes d'information d'importance vitale. Ces règles de sécurité s'appliquent notamment aux SIIV opérés par les sous-traitants.

Retrouvez ci-dessous une présentation synthétique et générique des règles de sécurité.

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Objectifs

- Porter les enjeux SSI au plus haut niveau de l'entité.
- Encourager l'opérateur à définir une stratégie SSI.

Elaboration et mise en œuvre d'une PSSI élaborée selon les critères définis par l'ANSSI, prévoyant notamment des plans de formation et de sensibilisation à la SSI.

Ressources : Guide d'élaboration de PSSI↗, norme ISO 27001↗, PSSIE

HOMOLOGATION DE SÉCURITÉ

Objectifs

- Identifier les risques portant sur les SIIV et les mesures adaptées pour les couvrir.
- Accepter formellement les risques résiduels, au niveau de responsabilité suffisant.

Homologation obligatoire pour chaque SIIV, prononcée par l'opérateur, incluant un audit réalisé selon les critères définis par l'ANSSI.

Ressources :
Guide « L'homologation de sécurité en neuf étapes simples »↗, référentiel PASSI↗

CARTOGRAPHIE

Objectifs

- Pouvoir apprécier l'impact d'une compromission.
- Faciliter le traitement des incidents de sécurité.
- Pouvoir qualifier et attribuer des signalements remontés par des partenaires de l'ANSSI.

Tenue à disposition de l'ANSSI d'une cartographie de chaque SIIV.

MAINTIEN EN CONDITIONS DE SÉCURITÉ

Objectifs

- S'assurer que les SIIV conservent un niveau de sécurité constant, adapté à l'évolution de la menace.

Suivi et prise en compte des correctifs de sécurité.

Gestion des mises à jour des SIIV.

JOURNALISATION

Objectifs

- Enregistrer les évènements permettant de détecter des incidents de sécurité.
- Pouvoir réaliser des investigations a posteriori en cas d'incident.
- Pouvoir réaliser des recherches de compromission.

Mise en place d'un système de journalisation pour chaque SIIV.

Ressources :
Note technique Prérequis à la mise en œuvre d'un système de journalisation

DÉTECTION

Objectifs

- Détecter au plus tôt les tentatives d'attaque.
- Pouvoir réagir rapidement en cas de compromission.

Mise en œuvre d'un système de corrélation et d'analyse des journaux, exploité en s'appuyant sur les exigences du référentiel PDIS.

Mise en œuvre de systèmes de détection qualifiées opérées par l'ANSSI, d'autres services de l'Etat ou des prestataires qualifiés, positionnées de manière à pouvoir analyser les flux échangés entre les SIIV et les autres systèmes.

Ressources :
Référentiel PDIS
Sonde réseau de détection des incidents de sécurité – Cible de sécurité

TRAITEMENT DES INCIDENTS DE SÉCURITÉ

Objectifs

- Assurer la gestion et la supervision des incidents.
- Mettre en place les ressources adaptées à l'analyse et au traitement de ces incidents.

Mise en place d'une organisation de gestion des incidents de sécurité informatique.

Traitement des incidents de sécurité en s'appuyant sur les exigences du référentiel PRIS.

Ressources :
référentiel PRIS

TRAITEMENT DES ALERTES

Objectifs

- Informer au plus vite l'opérateur d'un risque de compromission sur ses SIIV.
- Pouvoir activer rapidement des mesures de réaction en vue de limiter le périmètre de compromission et les impacts.

Communication à l'ANSSI d'un point de contact fonctionnel pouvant prendre connaissance à toute heure des signalements de l'ANSSI.

GESTION DE CRISES

Objectifs

- Préparer l'opérateur à activer les mesures de crise décidées par le Premier ministre.

Mise en œuvre d'une procédure de gestion de crise en cas d'attaques informatiques majeures.

GESTION DES IDENTITÉS ET DES ACCÈS

Objectifs

- Limiter l'exposition des SIIV aux attaques et aux erreurs de manipulation.
- Assurer la traçabilité des accès aux ressources des SIIV.

Identification par comptes individuels.

Protection des éléments secrets d'authentification.

Gestion des autorisations selon le principe du moindre privilège.

Connaissance des comptes privilégiés et des droits associés.

Ressources :
Note technique Sécurité des mots de passe

ADMINISTRATION

Objectifs

- Prévenir les attaques pouvant conduire à une prise de contrôle totale et furtive du SIIV.

Utilisation de comptes dédiés à l'administration pour l'administration des SIIV.

Mise en place de ressources matérielles et logicielles dédiées aux opérations d'administration.

Séparation entre les flux d'administration et les autres flux.

Ressources :
Note technique Sécuriser l'administration des SI

DÉFENSE EN PROFONDEUR

Objectifs

- Empêcher, a minima, ralentir toute attaque.
- Décourager les attaquants par l'investissement à consacrer pour mener une attaque.

Cloisonnement entre les différentes parties du SIIV et vis-à-vis des systèmes extérieurs au SIIV.

Application d'une politique de filtrage pour s'assurer que seuls les flux strictement nécessaires sont utilisés.

Contrôle strict des connexions distantes.

Durcissement des éléments du SIIV.

Ressources :
Ensemble des notes techniques, Guide des bonnes pratique

INDICATEURS

Objectifs

- Mieux évaluer le degré d'exposition des SIIV aux attaques informatiques.
- Affiner la stratégie de protection des opérateurs de chaque secteur.

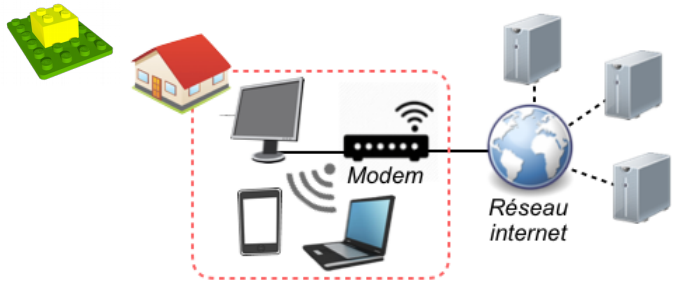
Evaluation pour chaque SIIV d'indicateurs SSI et transmission annuelle à l'ANSSI d'un tableau de bord de suivi de ces indicateurs.

Source : https://disciplines .ac-toulouse.fr/ sii/sites/sii.disciplines.ac-toulouse.fr/ files/ techno_college/cycle4/fc-cycle4/ip/ip11-1_architecture-reseau-internet.pdf

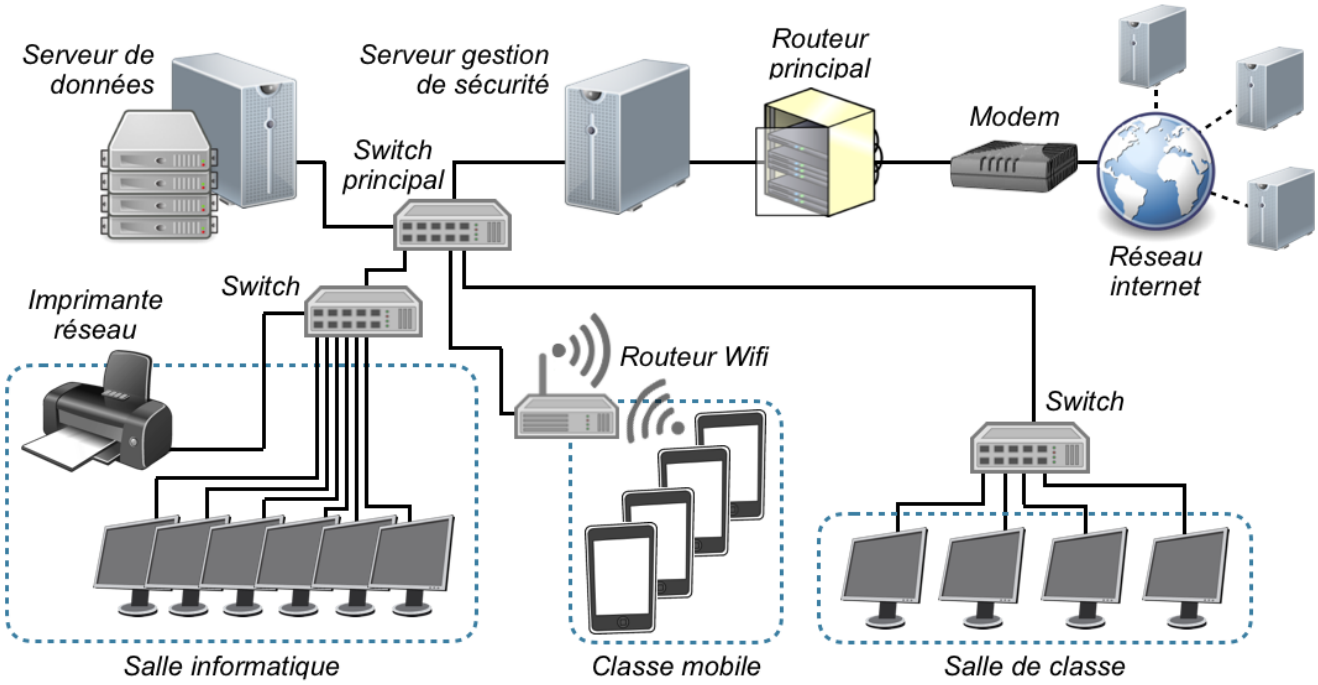
DOCUMENT 4

TECHNOLOGIE *Ce que je dois retenir*	ARCHITECTURE D'UN RÉSEAU ET INTERNET	CYCLE 4
CS 5.6 IP 1.1	Comprendre le fonctionnement d'un réseau informatique	

Architecture d'un réseau



Contrairement à l'installation simple que nous pouvons retrouver à la maison, l'architecture **d'un réseau local** s'impose au collège comme dans toutes entreprises qui utilisent des moyens numériques.



Composants principaux d'un réseau

Le modem permet une connexion à internet. C'est une interface entre le réseau et l'extérieur (câble téléphonique ou fibre optique).

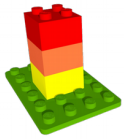
Le routeur permet de relier plusieurs réseaux locaux ensemble.
Il est présent dans **une baie de brassage** : armoire technique qui centralise les connexions du réseau local.

Un serveur permet de :
- Gérer les autorisations des utilisateurs
- Stocker les données des utilisateurs
- Gérer la sécurité des données qui transitent entre internet et le réseau ainsi qu'au sein du réseau lui même (firewall).

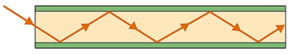
Le switch (commutateur) permet de relier plusieurs équipements (poste informatique, imprimante, …) au sein du réseau local.

Le routeur Wifi permet tout comme le switch de relier plusieurs équipements mais avec une connexion sans fil en Wifi.
Pour cela, il génère un sous-réseau local qui lui est propre (d'où le mot routeur)

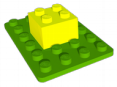
Moyens de connexion à un réseau



Actuellement il existe différents moyens de communication soit autant de connexion à un réseau. Cela permet d'optimiser la connexion de l'équipement au réseau local ou internet.
Le choix de la solution de connexion se fera en fonction de la nature mobile de l'équipement (appareil fixe ou mobile) et en fonction de la portée et de la rapidité souhaitée.

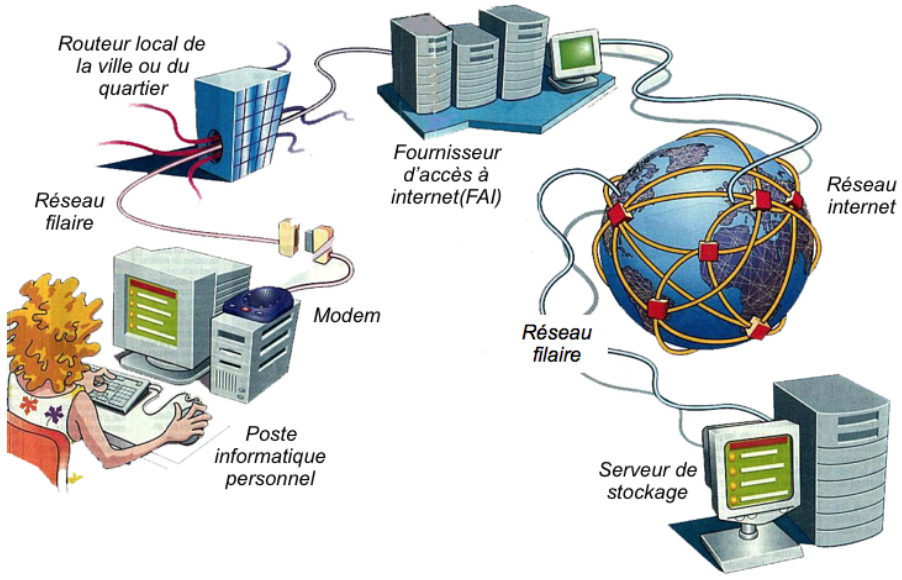
Moyen de connexion	Transmission du signal	Portée de la communication	Rapidité de communication	Nature du signal
 Câble ethernet	Filaire	☺ ☺ ☺	☺ ☺	Electrique
 Courant porteur en ligne (CPL)	Filaire	☺	☺ ☺	Electrique
 Fibre optique	Filaire	☺ ☺ ☺	☺ ☺ ☺	Impulsion lumineuse
 Wifi	Sans fil	☺	☺	Onde radio
 Bluetooth	Sans fil	☺	☺	Onde radio
 Li-Fi	Sans fil	☺	☺ ☺ ☺	Impulsion lumineuse infra-rouge
 Satellite	Sans fil	☺ ☺ ☺	☺	Onde radio

Un réseau mondial : Internet



Internet est un réseau de millions d'ordinateurs et d'objets interconnectés pour communiquer et échanger des informations. L'utilisateur se connecte à internet par son fournisseur d'accès à internet (FAI) qui lui fournit une adresse IP unique le temps de la connexion.

Chaque ordinateur ou équipement connecté à internet possède donc une adresse IP propre.
Des serveurs spécifiques font le lien entre une URL et une adresse IP.



Ainsi il est facile de se connecter avec son navigateur (firefox, chrome, internet explorer, …) à un serveur (qui stocke un site internet par exemple) avec uniquement l'adresse URL.

https://www.youtube.com

Exemple :
Youtube.fr = 173.194.40.110

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI-S_Guide_pratique_specifique_Wifi_V1.002.pdf

DOCUMENT 5

Guide pratique spécifique pour la mise en place d'un accès Wifi

Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)- Mai 2014 - V1.0

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

SOMMAIRE

Le présent document a été élaboré dans le cadre d'un processus collaboratif avec les principaux acteurs du secteur (institutionnels, utilisateurs et industriels) et le grand public.

La Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS) et l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) remercient l'ensemble des personnes et organisations qui ont apporté leur contribution à son élaboration et à sa relecture.

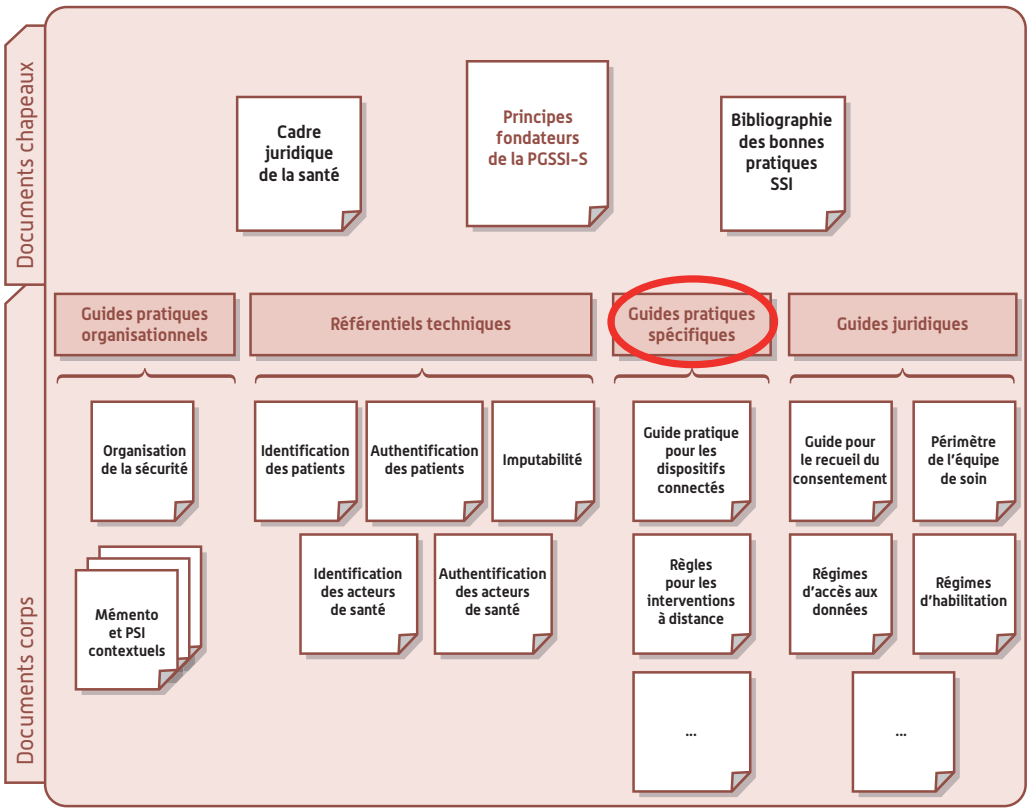
1. INTRODUCTION

1.1. Objet du document

Le présent document définit les règles de sécurité relatives à la mise en place d'un accès Wifi dans un Système d'Information de Santé (SIS).

Il fait partie des guides pratiques spécifiques de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

FIGURE 1 : PLACE DU DOCUMENT DANS LE CORPUS DOCUMENTAIRE DE LA PGSSI-S



Ce guide pratique exprime les règles de sécurité auxquelles doivent se conformer les responsables de Systèmes d'Information de Santé.

Les règles correspondent aux conditions requises et exposées dans les référentiels cités en référence pour que les risques sur la sécurité d'un SIS et les informations traitées restent acceptables lorsqu'un accès Wifi est mis en place dans ce système.

La mise en place d'un accès Wifi peut répondre à trois types de besoins :

1. Rendre possibles les accès sans fil, par des acteurs de santé, aux ressources informatiques.
   Ce besoin est principalement celui de professionnels de santé qui souhaitent s'affranchir de connexions filaires sur leur lieu d'exercice ou qui interviennent de manière intermittente sur divers lieux d'exercice.
   Ce cas est désigné par « accès PS » dans la suite du document.
2. Permettre à des équipements techniques du SIS de se connecter au réseau en mode Wifi.
   Ce besoin est principalement celui d'équipements connectés qui, pour des raisons d'usage en mobilité par exemple, tendent à privilégier progressivement la connectivité sans fil.
   Ce cas est désigné par « accès technique ».

3. Rendre possible des accès invités à des ressources tel l'accès Internet.
   Offrir à des patients (hospitalisés dans une structure de soins) ou encore des visiteurs (tous types d'organisation) la possibilité d'accéder à Internet avec des équipements Wifi sans risque supplémentaire pour le réseau du SIS.
   Ce cas est désigné par « accès invité ».
   Les employés d'une structure utilisant un « accès invité » sont considérés comme des utilisateurs externes dans le périmètre de cet accès. Le cas échéant, la charte d'utilisation des ressources de la structure peut limiter ou interdire l'utilisation de « l'accès invité » par les employés.

Ce document s'adresse :
- aux responsables de structure mettant en œuvre des accès Wifi ;
- aux personnes agissant sous leur responsabilité ; en particulier celles impliquées dans :
  - les processus d'acquisition des équipements et de leurs composantes informatiques,
  - les prestations d'exploitation,
  - les prestations de maintenances associées,
  - la mise en œuvre de la sécurité.

1.2. Champ d'application du document

Le document est applicable quels que soient les contextes de SIS rencontrés ou prévus et la structure juridique qui en est responsable, au sens des « Principes fondateurs de la PGSSI-S ».

Le cartouche ci-après présente de manière synthétique le périmètre d'application du document.

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

Les équipements suivants (liste non exhaustive) font partie du périmètre d'application du document :

Catégories	Exemples de ressources informatiques
Borne d'accès Wifi	Routeur/modem Wifi, points d'accès sans fil
Poste de travail	Ordinateur portable, tablette, …
Equipement éditique	Imprimante, photocopieur, scanner, …
Equipement téléphonique	Smartphone, téléphone portable, …
Equipement biomédical[1]	Appareil d'imagerie médicale, dispositif biomédical connecté, …

Limites du champ d'application :
Les dispositifs implantables[2] **et les dispositifs autonomes**[3] ne sont pas traités par le présent document. Il est toutefois possible de s'inspirer des règles présentées dans ce guide dans le cadre de la mise en œuvre de fonctionnalités sans fil de ce genre de dispositif.

Les accès wifi invité correspondant à des prestations commerciales offertes par des tiers et sans contact avec le SI de la structure ne sont pas traités dans le présent document. Il appartient au responsable de chacune de ces offres de sécuriser ces accès.

1. Au sens du Code de la Santé Publique (articles L 5211-1 et R 5211-1).
2. Dispositif médicaux destinés à être implantés en totalité ou partiellement dans le corps humain, de manière définitive ou pendant une période d'au moins 30 jours.
3. Équipements médicaux autonomes, c'est-à-dire dont l'usage et l'exploitation s'effectuent indépendamment de tout SIS.

1.3. Enjeux principaux relatifs aux accès Wifi

L'utilisation de réseaux Wifi procure un réel confort à l'utilisateur, puisqu'il permet de s'affranchir de la connexion physique des équipements au réseau local du SIS et ainsi répondre prioritairement aux besoins de mobilité.

En contrepartie, la mise en œuvre d'un tel réseau nécessite l'implémentation de mesures spécifiques de sécurité, car elle génère des risques de sécurité accrus sur le SIS.

En effet, l'installation d'un réseau sans fil sans mesure de sécurité spécifique peut permettre à des personnes non autorisées d'écouter et d'accéder au réseau interne du SIS qui contient des données de santé à caractère personnel.

En outre, la mise en place d'un accès Wifi ouvert aux invités (de type hot-spots) impose de respecter les règles relatives à la protection de la vie privée des utilisateurs de réseaux et services de communications électroniques explicitées dans les documents cités en référence de la PGSSI-S.

Des règles spécifiques peuvent s'appliquer aux bornes Wifi ouvertes au public, en particulier l'obligation de conservation des données de connexion (article L34-1 du code des postes et communications électroniques)[4].

Il est donc essentiel de définir des mesures de sécurité pour garantir :
- la confidentialité des données transmises sur la liaison Wifi ;
- le contrôle d'accès au SIS via l'accès Wifi ;
- le cloisonnement strict de l'accès invités vis-à-vis du SIS ;
- le respect de la réglementation en matière d'accès à Internet ouvert au public.

Par ailleurs, la disponibilité des communications Wifi doit être prise en compte. En effet, ce type de communications est particulièrement sensible à des attaques de type « déni de service », en particulier par brouillage des bandes de fréquence utilisées.

Il convient donc de prévoir un mode dégradé permettant de garantir la continuité des activités, notamment de production de soins, en cas de dysfonctionnement des communications Wifi.

4. En application de l'article L34-1 du Code des Postes et des Communications Électroniques, *« les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. »*

2. FONDEMENTS DU GUIDE

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié plusieurs notes concernant les réseaux Wifi sur lesquelles s'appuie le présent document :

- une note technique « Recommandations de sécurité relatives aux réseaux Wifi »[5] ;
- une Fiche Technique sur l'utilisation du Wifi (Portail de la sécurité informatique du 20 décembre 2007) ;
- une recommandation CERTA sur la sécurité des réseaux Wifi (21 novembre 2008 N° CERTA-2002-REC-002).

Les recommandations de ces documents sont reprises dans leurs principes par le présent document.

3. UTILISATION DU GUIDE

Les responsables identifiés au chapitre 1.1 sont en charge :

- de mettre en œuvre les règles prescrites ou de les faire appliquer par leurs sous-traitants ;
- d'estimer et de traiter les risques de sécurité induits par les règles non appliquées.

Le traitement d'un risque de sécurité peut consister à adopter une ou plusieurs des options suivantes vis-à-vis de ce risque :

- le réduire, par des mesures de protection ou de prévention ;
- l'accepter tel quel, notamment si le risque est jugé mineur par le responsable du SIS ;
- l'éviter, par exemple par le choix d'une connexion filaire plutôt que Wifi ;
- le transférer vers un tiers dans le cadre d'un contrat, étant précisé que cela n'exonère pas de toute responsabilité le responsable du SIS.

L'utilisation du guide s'effectue à partir de la liste des règles du chapitre suivant.

5. http://www.ssi.gouv.fr/IMG/pdf/NP_WIFI_NoteTech.pdf

4. RÈGLES POUR LA MISE EN PLACE D'UN ACCÈS WIFI

La totalité des règles ci-après est applicable dès la mise en œuvre d'un accès wifi. Il n'y a donc pas nécessité de distinguer des paliers de mise en œuvre.

N°	Règle	Applicabilité accès Wifi Invité
Installation et configuration d'un point d'accès Wifi		
[C1]	Seul le personnel ou les sociétés désignées par le responsable du SIS, ou leurs délégataires en charge de la gestion des réseaux informatiques, peuvent mettre en place et gérer un point d'accès Wifi. Une procédure d'installation et de sécurisation des points d'accès doit être formalisée. Elle doit être mise en œuvre lors de chaque installation d'un nouvel équipement.	X
[C2]	Le point d'accès Wifi doit être compatible avec la norme IEEE 802.11. Le choix des canaux de transmission du Wifi doit être effectué de manière à ne pas créer d'interférences avec d'autres équipements ou entre les différents réseaux wifi mis en œuvre (accès PS, accès technique et accès invité).	X
[C3]	Pour prévenir toute interférence potentielle, les recommandations des fournisseurs d'équipements de santé installés à portée du point d'accès Wifi doivent être respectées. Une étude doit être menée dans ce sens avant toute mise en œuvre de point d'accès Wifi.	X
[C4]	Le nombre de bornes, leur positionnement ainsi que la puissance du signal Wifi doivent être adaptés à la superficie de la zone à couvrir.	X
[C5]	Il convient de prévoir, pour les équipements connectés par Wifi un mode dégradé permettant de garantir la continuité des activités, en cas de dysfonctionnement des communications Wifi.	X
[C6]	Comme tous les équipements connectés au réseau, les équipements Wifi (bornes, câbles d'accès…) doivent, autant que faire se peut, être protégés et non accessibles au public afin d'éviter : • un accès direct au réseau interne du SIS, par exemple en déconnectant le câble de connexion et en l'utilisant directement sur son matériel ; • ou une réinitialisation non contrôlée de l'équipement. Cette protection peut être mise en œuvre par une combinaison de disposition physique et de configuration du matériel par exemple routeur wifi dans une boite fermée à clef, routeur wifi positionnée dans le champ de vision du personnel, désactivation des connecteurs RJ45 femelles non utilisés, authentification du routeur sur le réseau filaire…	X
[C7]	L'identifiant du réseau Wifi (SSID) doit être anonymisé afin d'éviter de faire apparaitre le nom de l'opérateur internet et de donner toute information qui permettrait à une personne mal intentionnée de se connecter au réseau. Il peut également être rendu invisible, nécessitant ainsi, lors de sa première connexion, que l'utilisateur entre manuellement les informations du SSID au lieu de la sélectionner dans la liste des réseaux. Il est cependant à noter que cette mesure n'est pas suffisante pour sécuriser l'accès au wifi, elle peut cependant réduire le nombre de tentatives de connexions frauduleuses.	X
[C8]	Un contrôle d'accès des équipements connectés au réseau interne du SIS via le Wifi doit être effectué. Il doit être réalisé en priorité par l'utilisation du protocole 802.1X[6]. Les réseaux Wifi et internes du SIS doivent être cloisonnés au moyen d'un dispositif de filtrage (firewall) n'autorisant que les services, les protocoles et les ports de communication nécessaires aux flux métiers prévus.	

6. Protocole standard lié à la sécurité des réseaux informatiques, il permet de contrôler l'accès aux équipements d'infrastructures réseau.

N°	Règle	Applicabilité accès Wifi Invité
[C9]	Les équipements utilisés pour se connecter (terminaux professionnels et équipements de santé) doivent être configurés, lors de leur installation, pour restreindre l'association automatique aux seuls réseaux Wifi légitimes et exigeant une authentification 802.1X dans le but d'éviter une connexion involontaire à un réseau malveillant qui se ferait passer pour un réseau légitime.	
[C10]	Le mot de passe par défaut du compte administrateur de la borne Wifi doit être modifié. Un mot de passe fort de 10 caractères au minimum (recours à la fois de caractères alphabétiques, numériques, spéciaux et non triviaux) doit être utilisé.	X
[C11]	Seuls les services, les protocoles et les ports de communication nécessaires au fonctionnement et à l'utilisation de la borne Wifi doivent être activés. Par exemple, le protocole DNS-SD doit notamment être désactivé quand le parc d'équipement ne nécessite pas de reconfiguration fréquente.	X
[C12]	L'authentification des utilisateurs et la confidentialité des données doivent être assurées par la mise en place de mécanismes s'appuyant sur la norme WPA2-entreprise (standard 802.1X et protocole EAP, idéalement EAP-TLS) avec utilisation de l'algorithme de chiffrement AES-CCMP. Le site de l'ANSSI décrit ces différents mécanismes (http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-liaisons-sans-fil/recommandations-de-securite-relatives-aux-reseaux-wifi.html). À défaut, le protocole PEAP/EAP-MSCHAPv2 peut être utilisé en lieu et place du protocole EAP-TLS.	
[C13]	Le certificat serveur présenté par le point d'accès Wifi configuré en WPA2-Entreprise doit être signé par une autorité de certification de confiance pour les postes clients.	
[C14]	Lorsque des mécanismes d'authentification robuste (802.1X) ne peuvent être utilisés, l'authentification des utilisateurs et la confidentialité des données doivent être assurées par le mode WPA2-PSK (WPA2-Personnel) avec utilisation de l'algorithme de chiffrement AES-CCMP. La clé de sécurité pour WPA2 doit être conforme aux règles d'élaboration de mots de passe non triviaux et changée dès l'installation puis régulièrement.	
[C15]	Les fonctions de simplification de l'authentification de type WPS (Wifi Protected Setup) doivent être désactivées.	X
[C16]	Un filtrage de l'accès aux sites web doit être mis en place conformément à la charte d'utilisation d'accès et d'usage du SIS de la structure.	X

N°	Règle	Applicabilité accès Wifi Invité
Exploitation d'un point d'accès Wifi		
[E1]	L'administration d'un point d'accès Wifi doit être réalisée depuis le réseau filaire interne du SIS, de préférence à partir d'un réseau d'administration logiquement séparé et en utilisant un protocole sécurisé (ex : HTTPS). Les interfaces d'administration du point d'accès ne doivent pas être disponibles depuis le réseau Wifi.	X
[E2]	Le micrologiciel de chaque point d'accès Wifi doit être maintenu et mis à jour régulièrement.	X
[E3]	Pour s'assurer de la compatibilité des matériels utilisés pour la mise en œuvre d'un point d'accès Wifi, des tests préalables doivent être réalisés.	X
[E4]	La gestion des traces doit être activée sur les points d'accès Wifi. Les traces doivent être centralisées et analysées régulièrement pour identifier des anomalies potentielles dans les accès effectués (heures d'accès, volumes de données échangées…). Les traces des points d'accès Wifi doivent être gérées selon les mêmes modalités que les autres traces générées par le SIS (ex. droits d'accès, durée de conservation…).	
[E5]	Le réseau du SIS ne doit pas accueillir de bornes Wifi non gérées par le responsable du SIS (ex. bornes Wifi « pirates »). Des contrôles doivent être menés régulièrement pour s'en assurer.	X
Mise en place d'un accès Wifi Invité		
[M1]	Le SIS interne doit être strictement cloisonné du réseau Wifi mis à disposition des invités pour ne pas permettre l'accès aux ressources du SIS interne. Dans l'idéal, l'accès invité doit disposer d'une infrastructure dédiée à cet usage, et ne donnant accès à aucune ressource du SIS interne. À défaut, un cloisonnement logique doit être mis en œuvre.	X
[M2]	L'accès Wifi Invité doit être conditionné soit par un code d'accès disponible à l'intérieur des locaux et changé régulièrement soit par un code personnel attribué de manière individuelle suite à une procédure d'enregistrement (accueil par exemple) soit éventuellement après enregistrement auprès d'un serveur/portail 802.1X ou d'un portail captif.	X
[M3]	Dans le cas où un code personnel est nécessaire pour l'accès Wifi invité, la procédure d'enregistrement doit comporter l'approbation par l'invité des conditions d'utilisation de l'accès Wifi Invité ou l'acceptation obligatoire de ces éléments lors de sa demande de connexion au réseau. Elle peut comporter la vérification et la consignation de l'identité du demandeur.	X
[M4]	Une trace des connexions Wifi des utilisateurs doit comporter les éléments suivants s'ils sont disponibles : • les informations permettant d'identifier l'utilisateur ; • les données relatives aux équipements terminaux de communication utilisés (par exemple adresse MAC, type d'équipement, adresse IP attribuée…) ; • les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication (protocole utilisé http, https, …) ; • les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; • les données permettant d'identifier le ou les destinataires de la communication (par exemple adresse IP ou nom DNS du site web consulté).	X
[M5]	La durée de connexion d'un invité doit être temporaire et sa durée explicitement indiquée lors de l'authentification au service. Dès lors que le délai est dépassé, la connexion wifi doit être automatiquement interrompue.	X

N°	Règle	Applicabilité accès Wifi Invité
[M6]	Des éléments de sensibilisation à la sécurité doivent être portés à la connaissance des « invités » utilisant le wifi notamment concernant le caractère public de l'accès mis à disposition, le fait qu'il n'est pas spécifiquement sécurisé par la structure hébergeant cet accès (ex. pas d'antivirus, pas de protection anti-intrusion des terminaux se connectant à l'accès wifi…) et les conditions d'usage (ex. engagement de sa responsabilité en cas de non-respect de la loi, existence éventuelle de mesure de filtrage et de trace des accès et des droits dont il dispose sur ce sujet…). Ces éléments peuvent par exemple être intégrée aux supports d'informations diffusés aux utilisateurs (ex. livret d'accueil, affiches en zone d'admission, dans les chambres et/ou dans les espaces patients internet, page d'accueil du portail d'accès au wifi…).	X
[M7]	Un filtrage doit être mis en place afin d'interdire l'accès aux sites web dont la consultation est interdite aux mineurs ou dont le contenu est illégal. Un filtrage plus contraignant peut être mis en place conformément à la charte d'utilisation d'accès et d'usage du SIS de la structure.	X

5. ANNEXES

5.1. Annexe 1 : Glossaire

Sigle / Acronyme	Signification
AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CERTA	Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques Informatiques
GT	Groupe de Travail
IPSec	Internet Protocol Security
MAC	Media Access Control
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PS	Personnel de Santé
PTS	Pôle Technique et Sécurité
SIS	Systèmes d'Information de Santé
SSID	Service Set Identifier
TLS	Transport Layer Security
WPA2	Wifi Protected Access
WPS	Wifi Protected Setup

5.2. Annexe 2 : Documents de référence

Référence nº 1 : Recommandations de sécurité relatives aux réseaux Wifi, (Note technique ANSSI, 30/03/2013)

Référence nº 2 : Fiche Technique sur l'utilisation du Wifi (ANSSI, 20/12/2007)

Référence nº 3 : Recommandation CERTA sur la sécurité des réseaux Wifi – Nº CERTA-2002-REC-002 (ANSSI, 21/11/2008)

Référence nº 4 : Corpus documentaire constituant la PGSSI-S (référentiels, guides pratiques et politiques contextuelles)

Référence nº 5 : Fiche pratique : « Conservation des données de trafic : hot-spots Wifi, cybercafés, employeurs, quelles obligations ? » (CNIL, 28/09/2010)

DOCUMENT 6

Source : https://www.ugap.fr/catalogue-marche-public/materiel-lan-wan-et-connectique-reseau_17253.html

Source : https://www.manager-go.com/gestion-de-projet/glossaire/cycle-de-vie-d-un-projet

Le cycle de vie du projet se décompose en 4 étapes principales

1 - Etape de cadrage

Cette première phase d'étude et d'analyse se nomme également : initialisation, démarrage ou encore avant-projet (avec des nuances dans le contenu suivant les approches utilisées).

Le projet est initialisé à partir d'un besoin (problème à résoudre ou opportunité à saisir), un objectif est défini, une analyse est menée pour identifier la meilleure façon de travailler sur la réponse à apporter.

> *Pour certains projets, des options de solution peuvent être évoquées dans un "business case". Une étude de faisabilité est alors menée pour choisir l'axe de travail.*

Cette phase entérine la décision de lancer le projet ou non (**GO ou NO GO**). Dans le cas positif, si ce n'est pas fait, le chef de projet et son équipe sont nommés, les principaux livrables sont définis.

2 - Etape de conception et de planification

L'équipe projet définit dans le détail ce qui doit être fait, comment et avec quels moyens. Elle planifie dans le temps les étapes et la mobilisation de ressources.

Le chef de projet affine en particulier le budget financier en intégrant les différentes charges : prestations externes, support interne (lorsque des refacturations entre services sont appliquées), les moyens matériels et les autres achats.

Tous ces éléments sont consignés dans un plan projet comprenant :

- une liste des grandes phases
- les activités à mener, les dépendances entre les tâches et les différents jalons à travers un diagramme de Gantt
- les livrables ,
- un plan de communication projet ,
- un plan de gestion des risques.

En complément, un plan qualité peut être construit afin de maîtriser le processus et ses livrables.

3 - Etape de réalisation du projet

Il s'agit de la mise en oeuvre concrète des éléments planifiés. Séances créatives , ateliers de travail , analyse de la valeur... le groupe projet oeuvre dans la recherche et déploiement de solutions pour satisfaire les objectifs définis.

Le chef de projet contrôle l'avancée des activités, le respect du planning, des dépenses, des résultats au regard du plan projet initial et l'ajuste si nécessaire. Il suit attentivement le tableau de bord agrégeant les principaux indicateurs clés de performance (KPI) pour s'assurer que l'exécution du projet reste dans les clous.

Régulièrement, il communique avec les parties prenantes : il les tient informées de l'avancée du projet et de toute dérive majeure.

Une fois toutes les opérations réalisées et validées, le client interne ou externe prend possession des livrables : livraison de solution, formation, etc.

4 - Etape de clôture

C'est l'heure du bilan et de l'organisation de la fin des travaux. Avec un l'objectif : capitaliser sur l'expérience récemment acquise.

Il est important de conclure proprement en organisant une réunion dédiée avec les principaux acteurs impliqués : parties prenantes, équipe projet, utilisateurs clés...

Puis en rédigeant un bilan de synthèse pour garder en mémoire les points forts, les points faibles et les leçons à tirer de cette nouvelle expérience

Diagramme de Gantt simplifié (non automatique)

BpE documents SOLUTIONS EXCEL

Intitulé du projet :

Date :

	Détail des tâches	Livrables	Ressources	Responsable
1	**Intitulé tâche**	**Livrables**	**Jours-hommes**	**Responsable**
1.1	Sous-tâche			
1.2	Sous-tâche			
1.3	Sous-tâche			
2	**Intitulé tâche**	**Livrables**	**Jours-hommes**	**Responsable**
2.1	Sous-tâche			
2.2	Sous-tâche			
2.3	Sous-tâche			
3	**Intitulé tâche**	**Livrables**	**Jours-hommes**	**Responsable**
3.1	Sous-tâche			
3.2	Sous-tâche			
3.3	Sous-tâche			
4	**Intitulé tâche**	**Livrables**	**Jours-hommes**	**Responsable**
4.1	Sous-tâche			
4.2	Sous-tâche			
4.3	Sous-tâche			
5	**Intitulé tâche**	**Livrables**	**Jours-hommes**	**Responsable**
5.1	Sous-tâche			
5.2	Sous-tâche			
5.3	Sous-tâche			
6	**Intitulé tâche**	**Livrables**	**Jours-hommes**	**Responsable**
6.1	Sous-tâche			
6.2	Sous-tâche			
6,3	Sous-tâche			
7	**Intitulé tâche**	**Livrables**	**Jours-hommes**	**Responsable**
7.1	Sous-tâche			
7.2	Sous-tâche			
7.3	Sous-tâche