MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS

Liberté
Égalité
Fraternité

EDE ISI 2

SESSION 2022

CONCOURS EXTERNE

CAPET, CAPET/CAFEP

Section : ÉCONOMIE ET GESTION

Option : INFORMATIQUE ET SYSTEMES D'INFORMATION

Épreuve écrite disciplinaire appliquée

Durée : 5 heures

Sont autorisés :

- *Le lexique SQL, sans commentaire ni exemple d'utilisation des instructions,*
- *La règle à dessiner les symboles informatiques.*

Sont interdits :

- *Les ouvrages de référence,*
- *Les dictionnaires,*
- *La calculatrice et tout matériel électronique (dont les montres connectées).*

- *Si vous repérez ce qui vous semble être une erreur d'énoncé, vous devez le signaler très lisiblement sur votre copie, en proposer la correction et poursuivre l'épreuve en conséquence.*
- *De même, si cela vous conduit à formuler une ou plusieurs hypothèses, vous devez la (ou les) mentionner explicitement.*

NB : Conformément au principe d'anonymat, votre copie ne doit comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé consiste notamment en la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de la signer ou de l'identifier.

Tournez la page S.V.P.

A

INFORMATION AUX CANDIDATS

Vous trouverez ci-après les codes nécessaires vous permettant de compléter les rubriques figurant en en-tête de votre copie.
Ces codes doivent être reportés sur chacune des copies que vous remettrez.

► **Enseignement public** :

Concours	Section/option	Epreuve	Matière
EDE	8031E	102	9312

► **Enseignement privé** :

Concours	Section/option	Epreuve	Matière
EDF	8031E	102	9312

Structure du sujet

Le sujet est composé de deux parties

Partie 1	Découverte du contexte organisationnel
Partie 2 (au choix)	2A – Approfondissement du contexte organisationnel STS SIO, option « Solutions d'infrastructure, systèmes et réseaux » - SISR
	2B – Approfondissement du contexte organisationnel STS SIO, option « Solutions logicielles et applications métiers » - SLAM

La documentation est structurée de la façon suivante

Dossier documentaire n°1 commun

Document 1.1	acquis des étudiants en première année de STS SIO
Document 1.2	environnement technologique mobilisable dans les laboratoires
Document 1.3	extraits du référentiel du BTS SIO
Document 1.4	contexte organisationnel de la clinique CMCO
Document 1.5	schéma simplifié du réseau de la clinique CMCO
Document 1.6	normes et règlements
Document 1.7	méthode « Expression des besoins et identification des objectifs de sécurité » adaptée aux données à caractère personnel
Document 1.8	risques liés à l'informatisation des données patient par l'exemple
Document 1.9	extrait de la fiche n°3 du guide pratique de la direction générale de l'offre des soins (DGOS) à destination des directeurs d'établissements de santé

Dossier documentaire n°2 spécifique à la partie 2A

Document 2.1	plan d'adressage du réseau de la clinique
Document 2.2	serveurs de la clinique CMCO
Document 2.3	description de l'application *Web* APPLI-ANES
Document 2.4	le pare-feu *Stomrshield Network Security*
Document 2.5	projet concernant la disponibilité de l'infrastructure
Document 2.6	haute disponibilité en informatique, définition concrète et conseils pratiques
Document 2.7	techniques améliorant la disponibilité

Dossier documentaire n°3 spécifique à la partie 2B

Document 3.1	RadiOne - Solution applicative de MediSoft
Document 3.2	MediSoft - Hébergeur de données de santé
Document 3.3	RadiOne - Extrait du schéma relationnel de la base de données clients de MediSoft
Document 3.4	RadiOne - Extrait du patron de conception modèle-vue-contrôleur (MVC)
Document 3.5	RadiOne - Extrait du diagramme de classes métier
Document 3.6	RadiOne - Extrait de la classe d'accès aux données PdoClients
Document 3.7	RadiOne - Maquette de recherche de spécialistes
Document 3.8	RadiOne - Maquette de connexion
Document 3.9	Top 10 des failles de sécurité des applications *Web*

Sujet : clinique maritime de la Côte d'Opale (CMCO)

Vous enseignez en section de techniciens supérieurs Services informatiques aux organisations (STS SIO). L'équipe pédagogique a choisi un contexte organisationnel qui sera utilisé dans les enseignements des blocs professionnels. Ce contexte permet de mettre les étudiantes et les étudiants en situation de participer, au sein de la clinique maritime de la Côte d'Opale (CMCO), à la mise en place d'un projet de certification "hébergeur de données de santé" (HDS).

À partir de vos connaissances et des ressources documentaires fournies, vous concevez une séquence pédagogique sur le thème « Analyse de risques et remédiations » décomposée en deux parties :

– la première partie, située en fin de première année de formation, doit permettre de formuler une proposition s'appuyant sur le contexte organisationnel afin de travailler des compétences communes du bloc de compétences **3 - Cybersécurité des services informatiques** ;

– la seconde partie située en début de deuxième année doit permettre de formuler une proposition exploitant le contexte afin d'approfondir les compétences de l'option de votre choix,

soit pour l'option « Solutions d'infrastructure, systèmes et réseaux» SISR (partie 2A) ;

soit pour l'option « Solutions logicielles et applications métiers » SLAM (partie 2B).

- - - -

Partie 1 – Découverte du contexte organisationnel

Dossier documentaire à exploiter : dossier n° 1 commun

Dans le cadre de l'enseignement commun du bloc de compétences **3 - Cybersécurité des services informatiques** du BTS SIO, vous avez à concevoir un scénario permettant la découverte du contexte pour travailler les compétences suivantes :

- **B3.1 Protéger les données à caractère personnel**
- **B3.4 Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques**

La situation et l'environnement d'apprentissage des étudiantes et étudiants, ainsi que le contexte « CMCO », sont présentés dans le dossier documentaire commun. Il s'agit de mettre les étudiantes et étudiants en situation d'analyser les vulnérabilités du système d'information de la clinique.

Travail à faire

Proposer une première partie de séquence pédagogique en précisant les points suivants :

– les objectifs d'apprentissage ;
– le déroulement : prérequis mobilisés, découpage en différentes phases, équipements ou technologies mobilisés ;
– les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
  - o les consignes fournies ou les éléments d'évaluation à traiter par les étudiantes et les étudiants ;
  - o la ou les ressources choisie(s) dans le dossier joint en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjonction d'indications, etc.) ;
  - o les attendus de chaque travail demandé aux étudiantes et aux étudiants.

En particulier, votre proposition intégrera la gestion des risques en vous appuyant sur la méthodologie « Expression des besoins et identification des objectifs de sécurité » (EBIOS) avec un prolongement sur la problématique de la confidentialité des échanges.

Partie 2A – Approfondissement du contexte organisationnel
STS SIO, option « Solutions d'infrastructure, systèmes et réseaux »

Vous choisissez de traiter cette partie ou la partie 2B.

Dossiers documentaires à exploiter : dossier n° 1 commun et dossier n°2 spécifique à la partie 2A

Vous assurez plus particulièrement l'enseignement des blocs de compétences **2 – Administration des systèmes et des réseaux** et **3 – Cybersécurité des services informatiques** du BTS SIO, pour les étudiantes et étudiants de l'option A « Solutions d'infrastructure, systèmes et réseaux » (SISR).

Dans le cadre de votre enseignement, vous décidez de poursuivre la séquence pédagogique pour travailler 3 à 4 sous-compétences parmi les suivantes :

- **B2.1A Concevoir une solution d'infrastructure réseau**
  - Analyser un besoin exprimé et son contexte juridique.
  - Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique.
  - Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue.
- **B2.2A Installer, tester et déployer une solution d'infrastructure réseau**
  - Installer et configurer des éléments nécessaires pour assurer la continuité des services.
  - Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure.
  - Tester l'intégration et l'acceptation d'une solution d'infrastructure.
- **B3.5A Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service**
  - Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure.
  - Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité.

Il s'agit de mettre les étudiantes et étudiants en situation de faire évoluer l'infrastructure réseau et système de la clinique suite à l'analyse des risques qui a montré des vulnérabilités.

Travail à faire

Proposer une seconde partie de séquence pédagogique en précisant les points suivants :

- les objectifs d'apprentissage ;
- le déroulement : prérequis mobilisés, découpage en différentes phases, équipements ou technologies mobilisés ;
- les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
  - les consignes fournies ou les éléments d'évaluation à traiter par les étudiantes et les étudiants,
  - la ou les ressources choisie(s) dans le dossier joint en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjonction d'indications, etc.),
  - les attendus de chaque travail demandé aux étudiantes et aux étudiants.

En particulier, votre proposition intégrera le thème de la disponibilité des services et de l'infrastructure réseau.

Partie 2B – Approfondissement du contexte organisationnel
STS SIO, option « Solutions logicielles et applications métiers »

Vous choisissez de traiter cette partie ou la partie 2A.

Dossiers documentaires à exploiter : dossier n° 1 commun et dossier n° 3 spécifique à la partie 2B

Vous assurez plus particulièrement l'enseignement des blocs de compétences **2 – Conception et développement d'applications** et **3 – Cybersécurité des services informatiques** du BTS SIO, pour les étudiantes et étudiants de l'option B « Solutions logicielles et applications métiers » (SLAM).

Dans le cadre de votre enseignement, vous décidez de poursuivre la séquence pédagogique pour travailler 3 à 4 sous-compétences parmi les suivantes :

- **B2.1B Concevoir et développer une solution applicative**
  - Modéliser une solution applicative
  - Participer à la conception de l'architecture d'une solution applicative
  - Identifier, développer, utiliser ou adapter des composants logiciels
  - Utiliser des composants d'accès aux données

- **B2.3B Gérer les données**
  - Exploiter des données à l'aide d'un langage de requêtes
  - Concevoir ou adapter une base de données
  - Développer des fonctionnalités applicatives au sein d'un système de gestion de bases de données (relationnel ou non)

- **B3.5B Assurer la cybersécurité d'une solution applicative et de son développement**
  - Participer à la vérification des éléments contribuant à la qualité d'un développement informatique
  - Prendre en compte la sécurité dans un projet de développement d'une solution applicative
  - Prévenir les attaques

Il s'agit de mettre les étudiantes et étudiants en situation de faire évoluer la solution applicative utilisée par la clinique et développée par l'entreprise de services du numérique (ESN) MediSoft, suite au besoin de nouvelles fonctionnalités et à l'analyse de risques qui a montré des vulnérabilités.

Travail à faire

Proposer une seconde partie de séquence pédagogique en précisant les points suivants :

- les objectifs d'apprentissage ;
- le déroulement : prérequis mobilisés, découpage en différentes phases, équipements ou technologies mobilisés ;
- les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
  - les consignes fournies ou les éléments d'évaluation à traiter par les étudiantes et les étudiants ;
  - la ou les ressources choisie(s) dans les dossiers joints en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjonction d'indications, etc.) ;
  - les attendus de chaque travail demandé aux étudiantes et aux étudiants.

En particulier, votre proposition permettra l'approfondissement de la programmation orientée objet (exploitation d'un diagramme de classes et son implémentation, modélisation et implémentation de l'héritage, parcours de collections, exploitation de cas d'utilisation) en traitant la gestion des failles de sécurité identifiées.

Dossier documentaire n° 1 commun

Document 1.1 : acquis des étudiants en première année de STS SIO

Ce document rassemble les acquis des étudiantes et étudiants lors de leur première année en section de techniciens supérieurs SIO, en termes de savoirs et de savoirs technologiques. Ces acquis sont mobilisables dans les scénarios pédagogiques des parties 1 et 2 (A et B).

Les compétences communes travaillées dans les blocs 1 - Support et mise à disposition de services informatiques et 3 - Cybersécurité des services informatiques ont permis d'aborder les notions suivantes :

- Modèle OSI et TCP/IP, adressage IPv4, protocoles Ethernet (y compris les réseaux sans fil),
- Notions de routage et de segmentation.
- Principaux protocoles et services associés : services d'annuaire (LDAP/Domaine AD), services *Web*, services d'architecture (DNS/DHCP), services de communication (partage de fichiers, messagerie, outils collaboratifs)
- Bases sur la résolution des incidents : processus de recueil de bonnes pratiques informatiques (ITIL), cycle de vie d'un incident
- Programmation procédurale, bases de la programmation orientée objet et de la programmation *Web*, langage de macrocommande (*script*).
- Notions sur le fonctionnement d'une base de données relationnelle et du langage SQL.
- Bases sur la protection des données personnelles et de l'identité numérique de l'organisation.
- Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.
- Principes et techniques sur la protection, la gestion des droits d'accès et l'archivage des données, le chiffrement, l'authentification et la preuve.
- Typologie des risques et de leurs impacts, initiation à l'analyse de risques.

Les étudiantes et étudiants ont une pratique courante des technologies suivantes :

- Bases de l'administration système sous Windows et Linux : commandes de base, consultation de fichiers, filtres, installation de paquets.
- Bases de l'administration réseau : mise à disposition d'un accès à un réseau.
- Installation, administration et sécurisation du poste de travail.
- Utilisation de l'outil de simulation *Cisco Packet Tracer* et d'équipements physiques : commutateurs, routeurs, points d'accès sans-fil (sécurisation par WPA2 PSK).
- Pratique d'un outil de gestion de projet (tâches, planification, ressources).
- Pratique d'un outil de gestion des incidents.
- Techniques de mise à disposition de site *Web* (local, nuage –*cloud*- privé, nuage –*cloud*- public).
- Étude et modification de site web (langage de macrocommande –*script*- client HTML, CSS, *Javascript*).
- Étude et modification de site PHP MySQL (langage de macrocommande –*script*- serveur et accès aux données).
- Étude et modification de site *Web* (système de gestion de contenus tel que *WordPress*).
- Interprétation et modification des formats de données structurées (JSON, XML).
- Génération et exploitation de scripts de création de base de données.
- Manipulation des données à l'aide du langage SQL.

Spécifiquement pour l'option SISR :
Les compétences travaillées dans le bloc 2 ont permis d'approfondir les principes et la mise en œuvre des architectures réseau et système : séparation des flux (réseaux virtuels – VLAN-, propagation de VLAN - 802.1q, zone démilitarisée – DMZ-, autres périmètres de sécurité, etc.), adressage IP, routage (avec routage dynamique), translation d'adresses réseau (NAT), accès distant, langage de script, déploiement de postes de travail et d'applications et administration d'un serveur *Windows* et/ou *Linux*.

Spécifiquement pour l'option SLAM :
Les compétences travaillées dans le bloc 2 ont permis d'approfondir les principes et la mise en œuvre de la programmation (notamment orientée objet) et des bases de données : modélisation et maquettage d'une solution applicative, architectures applicatives n-tiers, adaptation d'une base de données en réponse à de nouveaux besoins, accès aux données à travers des requêtes du langage de la base de données depuis une application et gestion de versions de code source.

Document 1.2 : environnement technologique mobilisable dans les laboratoires

Les différents laboratoires des options SISR et SLAM au sein desquels les enseignements se déroulent sont équipés d'environnements conformes à l'annexe 2E du référentiel du BTS SIO et décrits ci-après.

Environnement technologique mobilisable pour l'ensemble des blocs de compétences :

- un service d'authentification pour les utilisateurs internes et externes à l'organisation ;
- un SGBD ;
- un accès sécurisé à internet ;
- un environnement de travail collaboratif ;
- deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel open source ;
- une solution de sauvegarde ;
- des ressources dont l'accès est sécurisé et soumis à habilitation ;
- deux types de terminaux dont un mobile (type « *smartphone »* ou encore tablette) ;
- un outil de gestion des incidents ;
- des services exploitant des techniques de chiffrements.

Environnement technologique mobilisable pour l'option A « Solutions d'infrastructure, systèmes et réseaux » :

- un réseau comportant plusieurs périmètres de sécurité ;
- un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité ;
- un logiciel d'analyse de trames ;
- un logiciel de gestion des configurations ;
- une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès ;
- une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes ;
- une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet) ;
- une solution garantissant la continuité d'un service ;
- une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion ;
- une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion ;
- une solution permettant le déploiement d'un réseau filaire *Ethernet* commuté et *Wi-Fi* ;
- une solution permettant la connexion sécurisée entre deux sites distants ;
- une solution permettant le déploiement des solutions techniques d'accès ;
- une solution gérée à l'aide de procédures automatisées écrites avec un langage de script ;
- une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau.

Environnement technologique mobilisable pour l'option B « Solutions logicielles et applications métiers » :

- un ou deux environnements de développement disposant d'outils de gestion de tests et supportant un cadre applicatif (*framework*) et au moins deux langages ;
- une bibliothèque de composants logiciels ;
- un SGBD avec langage de programmation associé ;
- un logiciel de gestion de versions et de suivi de problèmes d'ordre logiciel ;
- une solution permettant de tester les comportements anormaux d'une application ;
- Au sein des architectures de ces solutions applicatives se retrouvent du code exécuté sur le système d'exploitation d'une solution technique d'accès fixe (type client lourd), du code exécuté dans un navigateur *Web* (type client léger ou riche) et du code exécuté sur le système d'exploitation d'une solution technique d'accès mobile.

Une solution applicative peut être issue d'un développement spécifique ou de la modification du code d'un logiciel notamment libre (*open source)*.

Source : extrait du référentiel du BTS Services informatiques aux organisations – Annexe 2E

Document 1.3 : extraits du référentiel du BTS SIO

Bloc 2 - Administration systèmes et réseaux options - Option A « Solutions d'infrastructure, systèmes et réseaux »

Compétences	Indicateurs de performances	Savoirs associés
B2.1A - Concevoir une solution d'infrastructure réseau • Analyser un besoin exprimé et son contexte juridique • Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique • Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue **B2.2A - Installer, tester et déployer une solution d'infrastructure réseau** • Installer et configurer des éléments nécessaires pour assurer la continuité des services • Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure • Tester l'intégration et l'acceptation d'une solution d'infrastructure	Les risques liés à une mauvaise utilisation ou à un dysfonctionnement de la solution d'infrastructure sont identifiés. Les composants de l'architecture technique sur lesquels la solution d'infrastructure à produire aura un impact sont recensés. Les éléments d'infrastructure permettant d'assurer la continuité de service sont installés et configurés. Le service fonctionne avec la disponibilité attendue. Une procédure de remplacement ou de migration d'un élément d'infrastructure est élaborée et mise en œuvre en respectant la continuité d'un service. L'intégration de la solution ne génère pas de dysfonctionnement du réseau ou dans le réseau.	Principes des architectures réseau : modèles de référence, normes et technologies, périmètres de réseau, routage, plans d'adressage. Outil de conception et de simulation d'architecture réseau : techniques, fonctionnalités et paramétrage. Installation et configuration des éléments d'interconnexion et des services techniques réseau. Déploiement d'éléments d'infrastructure : méthodes, technologies, techniques, normes et standards associés Techniques, outils et protocoles d'administration à distance. Langage de commande d'un système d'exploitation : commandes et script d'administration d'une solution d'infrastructure. Disponibilité des services, des systèmes, des serveurs et des infrastructures réseaux : méthodes, technologies, techniques, normes et standards associés. Mise en œuvre des solutions permettant d'atteindre les niveaux de disponibilité et de qualité de service à plusieurs niveaux. Plans de continuité et de reprise d'activité.

Tournez la page S.V.P.

Bloc 2 - Solutions logicielles et applications métiers- Option B « Solutions logicielles et applications métiers »

Compétences	Indicateurs de performance	Savoirs associés
B2.1B - Concevoir et développer une solution applicative • Analyser un besoin exprimé et son contexte juridique • Participer à la conception de l'architecture d'une solution applicative • Modéliser une solution applicative • Identifier, développer, utiliser ou adapter des composants logiciels • Utiliser des composants d'accès aux données • Réaliser les tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés • Intégrer en continu les versions d'une solution applicative **B2.3B - Gérer les données** • Exploiter des données à l'aide d'un langage de requêtes • Développer des fonctionnalités applicatives au sein d'un système de gestion de base de données (relationnel ou non) • Concevoir ou adapter une base de données • Administrer et déployer une base de données	Le choix des composants logiciels à utiliser et/ou à développer est pertinent. Les composants logiciels sont validés par les procédures de tests unitaires et fonctionnels. Les données persistantes liées à la solution applicative sont exploitées à travers un langage de requête lié à la base de données qui peut être le langage de requête proposé par les échanges applicatifs des technologies Web, un langage de requête présent dans l'outil de correspondance objet-relationnel ou toute autre solution de persistance. L'application développée est opérationnelle conformément au cahier des charges et stable dans l'environnement de production. Les tests d'intégration sont réalisés. Un outil collaboratif de gestion des itérations de développement et de versions est utilisé. Une documentation des versions vient appuyer l'intégration continue. L'exploitation des données permet de construire l'information attendue. Les accès aux données sont contrôlés conformément aux habilitations définies par le cahier des charges. Les données sont modélisées conformément au besoin de la solution applicative.	Méthodes, normes et standards associés au processus de conception et de développement d'une solution applicative. Architectures applicatives : concepts de base et typologies. Techniques et outils d'analyse et de rétro-conception. Concepts de la programmation objet : classe, objet, abstraction, interface, héritage, polymorphisme, annotations, patrons de conception, interface de programmation d'applications. Persistance et couche d'accès aux données. Fonctionnalités d'un outil de gestion de projets. Concepts et techniques de développement agile.

Bloc 3 - Cybersécurité des services informatiques

Compétences	Indicateurs de performance	Savoirs associés
B3.1 - Protéger les données à caractère personnel • Recenser les traitements sur les données à caractère personnel au sein de l'organisation. • Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel. **B3.4 - Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques.** • Caractériser les risques liés à l'utilisation malveillante d'un service informatique • Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité **B3.5A - Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service.** • Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure. • Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité.	La collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur. La charte informatique contient des dispositions destinées à protéger les données à caractère personnel. Le recensement des traitements des données à caractère personnel est exhaustif. Des moyens de protection sont mis en place pour garantir la confidentialité et l'intégrité des données personnelles en tenant compte des risques identifiés. Les risques associés à l'utilisation malveillante d'un service informatique sont caractérisés. Les conséquences des actes malveillants sur un service informatique sont identifiées. Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées : • un schéma présentant la segmentation du réseau est disponible ; • les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ; • l'authentification et la confidentialité des échanges sont vérifiées ; • la sécurité de l'administration est prise en compte ; • les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ; • les accès aux données sont contrôlés à chaque étape d'une transaction ; • les systèmes et les applications sont actualisés en fonction des alertes de sécurité ; • les vulnérabilités connues sont contrôlées.	Typologie des risques et leurs impacts. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. Authentification, privilèges et habilitations des utilisateurs : principes et techniques. Gestion des droits d'accès aux données : principes et techniques. Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique. Protection et archivage des données : principes et techniques. Chiffrement, authentification et preuve : principes et techniques. Sécurité des applications Web : risques, menaces et protocoles. Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique. Sûreté des infrastructures réseaux : bonnes pratiques, normes et standards. Cybersécurité : bonnes pratiques, normes et standards. Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services. Outils de sécurité : prévention et détection des attaques, gestion d'incidents.

Tournez la page S.V.P.

Bloc 3 - Cybersécurité des services informatiques (suite)

Compétences	Indicateurs de performance	Savoirs associés
B3.5B - Assurer la cybersécurité d'une solution applicative et de son développement ▪ Participer à la vérification des éléments contribuant à la qualité d'un développement informatique ▪ Prendre en compte la sécurité dans un projet de développement d'une solution applicative ▪ Prévenir les attaques	Le respect des bonnes pratiques de développement informatique est vérifié (les structures de données sont normalisées, les accès aux données sont optimisés, le code est modulaire et robuste, les tests sont effectués). Les préoccupations de sécurité sont prises en compte à toutes les étapes d'un développement informatique. Les bonnes pratiques de sécurité sont mises en œuvre à toutes les étapes d'un développement informatique. Des tests de sécurité sont prévus et mis en œuvre. Les traitements sur les données à caractère personnel sont déclarés et respectent la réglementation. Le système d'authentification est conforme aux règles de sécurité. L'accès aux données respecte les règles de sécurité. Les échanges de données entre applications sont protégés. Les composants utilisés sont certifiés, sécurisés et actualisés. Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité. Les contre-mesures sont documentées de manière à en assurer le suivi. La communication écrite et orale est adaptée à l'interlocuteur.	Développement informatique : méthodes, normes, standards et bonnes pratiques. Aspects réglementaires du développement applicatif : protection de la vie privée dès la conception, protection des données par défaut, sécurité par défaut, droit des individus. Sécurité du développement d'application : gestion de projet, architectures logicielles, rôle des protocoles, authentification, habilitations et privilèges des utilisateurs, confidentialité des échanges, tests de sécurité, audit de code. Vulnérabilités et contre-mesures sur les problèmes courants de développement. Environnements de production et de développement : fonctionnalités de sécurité, techniques d'isolation des applicatifs. .

Document 1.4 : contexte organisationnel de la clinique CMCO

La clinique maritime de la Côte d'Opale (CMCO) fait partie du groupement de cliniques du nord (GCN) créé en 1970 et constitué de 10 établissements. Une direction des systèmes d'information (DSI) est mutualisée au sein du groupement.

L'ensemble des cliniques sont certifiées ISO 27001 et ont pour objectif la certification d'hébergement des données de santé (HDS), même si cela n'est pas une obligation.

La clinique CMCO est un établissement pluridisciplinaire accueillant chaque année plus de 20 000 séjours dans 240 lits.

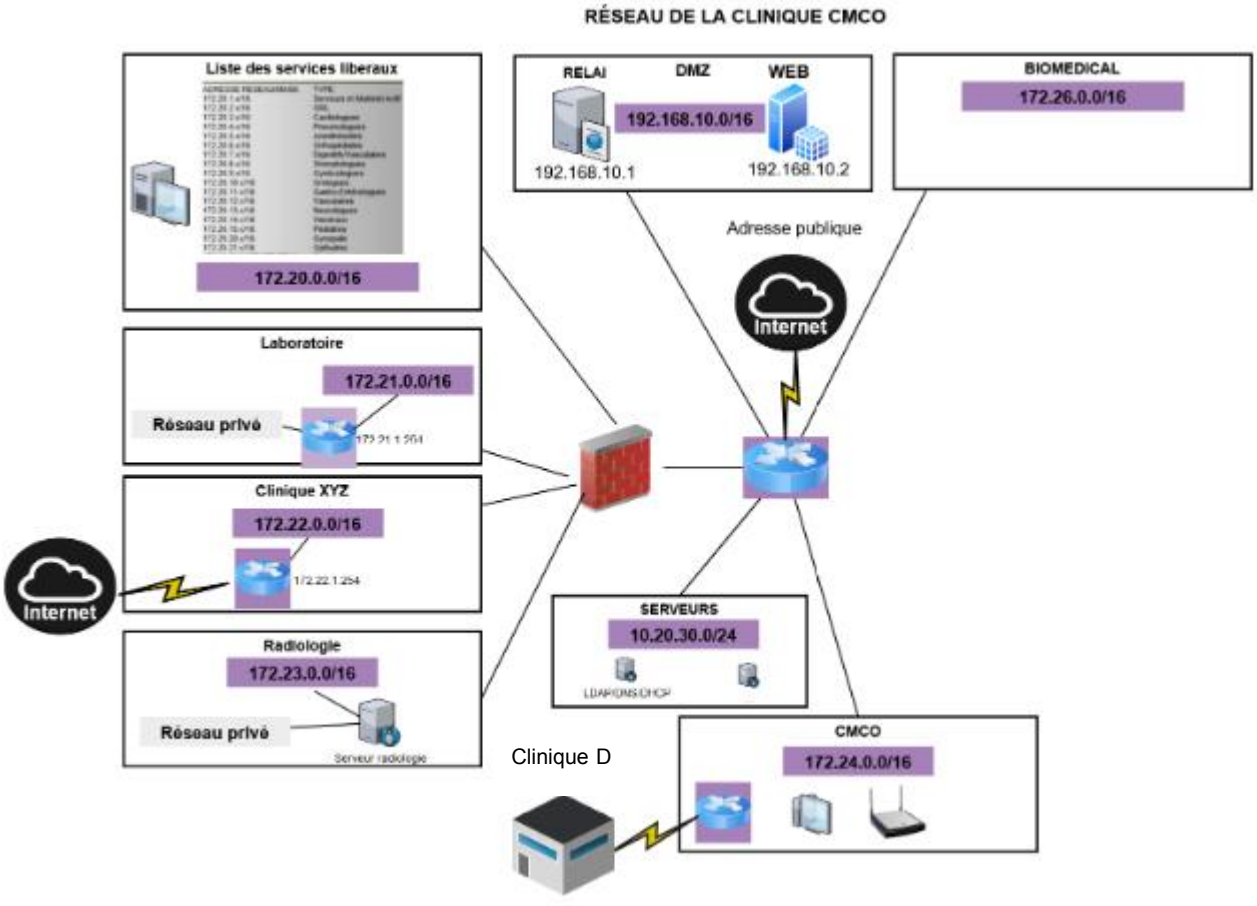
Le système d'information de la clinique est potentiellement soumis à de nombreuses vulnérabilités d'origines diverses : structures organisationnelles insuffisamment robustes, routines de gestion ou procédures défaillantes, pannes d'équipements, environnement physique mal contrôlé, multiplicité des intervenants, dépendance à des tiers défaillants, assemblage de composants dont la compatibilité n'est pas garantie, défaillance humaine, etc.

Ces vulnérabilités, si elles sont « exploitées », peuvent avoir des conséquences plus ou moins dommageables pour l'établissement en termes de temps de travail, de perte d'information, de coût financier, d'image de marque ou encore de réputation.

Dans le cadre du projet de certification « hébergeur de données de santé » (HDS), un audit interne est réalisé. Les priorités retenues pour celui-ci sont :

- la gestion des données à caractère personnel ;
- l'adéquation des technologies et des périphériques disponibles avec les besoins de sûreté et de sécurité : disponibilité, intégrité, confidentialité et preuve.

Document 1.5 : schéma simplifié du réseau de la clinique CMCO



Tournez la page S.V.P.

Document 1.6 : normes et règlements

La norme ISO 27001 *(d'après www.oceanet-technology.com)*

La certification ISO 27001 est de plus en plus intégrée dans les nouveaux référentiels, comme par exemple l'hébergement de données de santé. La norme internationale, nommée « Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences » a pour particularité de traiter la sécurité par les risques. Une entreprise certifiée ISO 27001 montre qu'elle a conscience des risques pesant sur ses données sensibles, qu'elle les prend en compte et qu'elle s'en protège.

Il ne s'agit pas seulement de protections physiques ou informatiques. La mise en œuvre de la certification ISO 27001 a bien pour objectif de protéger l'entreprise de toute perte, vol ou altération de données, mais pas uniquement en défendant les systèmes informatiques contre les intrusions ou les sinistres. La norme donne des bonnes pratiques conceptuelles qui viennent compléter ces mesures techniques, pour une sécurité à 360 degrés.

Ce périmètre global, à la fois technique et organisationnel, est appelé le système de management de la sécurité de l'information (SMSI). Il regroupe les systèmes d'information, les processus et les personnes qui sont concernées par les mesures de protection. La norme ISO 27001, en réalité, fournit donc un cadre permettant de mettre en place, d'exploiter et de faire évoluer ce SMSI dans le contexte d'une organisation.

La norme hébergement de données de santé – HDS *(extrait de esante.gouv.fr)*

La procédure de certification repose sur une évaluation de conformité au référentiel de certification. L'hébergeur choisit un organisme certificateur qui devra être accrédité par le comité français d'accréditation (COFRAC ou équivalent au niveau européen). L'organisme procède à un audit en deux étapes pour évaluer la conformité de l'hébergeur aux exigences du référentiel de certification. Il vérifie notamment l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000 déjà obtenues par l'hébergeur.

Étape 1 : audit documentaire. L'organisme certificateur réalise une revue documentaire du système d'information de l'organisation candidate afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification.

Étape 2 : audit sur site. Les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation. L'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles non-conformités et faire auditer ses corrections. Passé ce délai et sans action de l'hébergeur, toute la procédure d'audit sur site sera de nouveau réalisée.

Le règlement général sur la protection des données (RGPD) appliqué aux données de la santé

Le règlement général sur la protection des données (RGPD) donne une définition des données de santé et fixe le cadre de leur protection.

Le RGPD définit, dans son article 4, ce que sont **les données à caractère personnel concernant la santé** : il s'agit de « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

Il précise qu'elles devraient comprendre « *toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'une clinique, d'un dispositif médical ou d'un test de diagnostic in vitro* ».

Il définit aussi les **données génétiques**, « *relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé* », et les **données biométriques**, « *résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique* ».

Document 1.7 : méthode « Expression des besoins et identification des objectifs de sécurité » adaptée aux données à caractère personnel (*Extrait de cnil.fr)*

La méthode **Expression des besoins et identification des objectifs de sécurité** (EBIOS) vise à évaluer la gravité et la vraisemblance des données à caractère personnel.

Gravité

Afin de hiérarchiser les événements redoutés, la gravité est déterminée en fonction du caractère identifiant des données à caractère personnel (DCP) et du caractère préjudiciable de ces impacts potentiels. Tout d'abord, le caractère identifiant de l'ensemble des DCP (précédemment identifiées) doit donc être estimé : avec quelle facilité peut-on identifier les personnes concernées ?

1. Négligeable : il semble quasiment impossible d'identifier les personnes à l'aide des DCP les concernant (ex. : prénom seul à l'échelle de la population française).
2. Limité : il semble difficile d'identifier les personnes à l'aide des DCP les concernant, bien que cela soit possible dans certains cas (ex. : nom et prénom à l'échelle de la population française).
3. Important : il semble relativement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom et date de naissance, à l'échelle de la population française).
4. Maximal : il semble extrêmement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom, date de naissance et adresse postale, à l'échelle de la population française).

Ensuite, leur caractère préjudiciable doit être estimé pour chaque événement redouté : quelle serait l'importance des dommages correspondant à l'ensemble des impacts potentiels ? :

1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement...).
2. Limité : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...).
3. Important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...).
4. Maximal : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès...).

Enfin, la gravité est déduite en fonction des valeurs retenues pour le caractère identifiant des DCP et le caractère préjudiciable des impacts. Elle se détermine en additionnant les deux valeurs et en identifiant la gravité correspondante dans le tableau suivant :

Caractère identifiant + caractère préjudiciable	Gravité correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

Tableau 1 - Détermination de la gravité de chaque événement redouté

Il est possible d'augmenter ou de diminuer la gravité ainsi déduite en tenant compte d'autres facteurs. Par exemple, un grand nombre de personnes concernées (ce qui peut favoriser un sinistre massif) pourrait augmenter la gravité d'un niveau. Un grand nombre d'interconnexions (notamment avec l'étranger) ou de destinataires (ce qui facilite la corrélation de DCP initialement séparées) pourrait également être considéré comme un facteur aggravant. À contrario, très peu de personnes concernées, pas ou très peu d'interconnexions ou de destinataires, pourraient diminuer la gravité d'un niveau.

Vraisemblance

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de toutes les menaces qui permettraient aux événements redoutés de survenir. Il est possible de ne pas étudier celles qui concernent les événements redoutés dont la gravité est négligeable (1) ou limitée (2). Une menace étant une action possible des sources de risques sur les supports, il convient d'identifier et d'estimer ces éléments pour chaque menace.

La vraisemblance est directement liée à la vulnérabilité des supports et les capacités des attaquants à les exploiter.

Tout d'abord, les vulnérabilités des supports sont estimées pour chaque menace : dans quelle mesure les caractéristiques des supports sont-elles exploitables pour réaliser la menace ? :

1. Négligeable : il ne semble pas possible de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
2. Limité : il semble difficile de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
3. Important : il semble possible de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).
4. Maximal : il semble extrêmement facile de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

Des mesures existantes ou prévues peuvent avoir pour effet de réduire les vulnérabilités des supports.

Ensuite, les capacités des sources de risques sont estimées pour chaque menace : quelles sont leurs capacités à exploiter les vulnérabilités (compétences, temps disponible, ressources financières, proximité du système, motivation, sentiment d'impunité...) ? :

1. Négligeable : les sources de risques ne semblent pas avoir de capacités particulières pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges restreints).
2. Limité : les sources de risques ont quelques capacités, mais jugées peu importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges restreints).
3. Important : les sources de risques ont des capacités réelles, jugées importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges d'administration illimités).
4. Maximal : les sources de risques ont des capacités certaines, jugées illimitées, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges d'administration illimités). On retient la valeur dont la description correspond le mieux aux sources de risques identifiées.

Des mesures existantes ou prévues peuvent avoir pour effet de réduire les capacités des sources de risques.

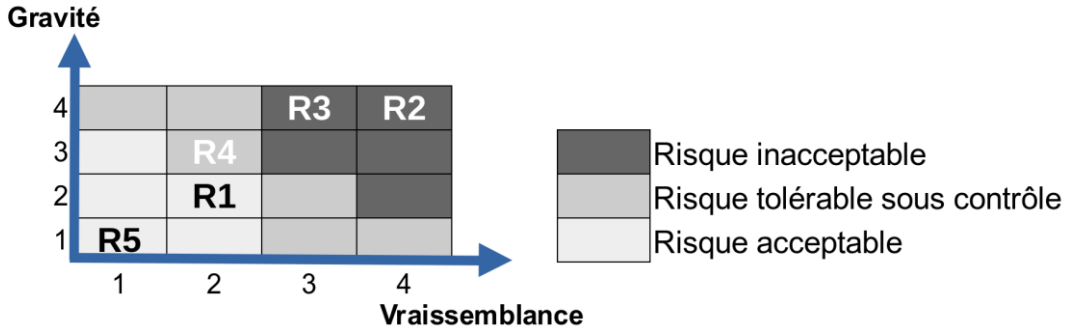
Enfin, la vraisemblance des menaces est déduite, en fonction des valeurs retenues pour les vulnérabilités des supports et les capacités des sources de risques. Elle se détermine en additionnant les deux valeurs et en identifiant la vraisemblance correspondante en se reportant au tableau suivant :

Vulnérabilités des supports + capacités des sources de risques	Vraisemblance correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

Évaluation des risques

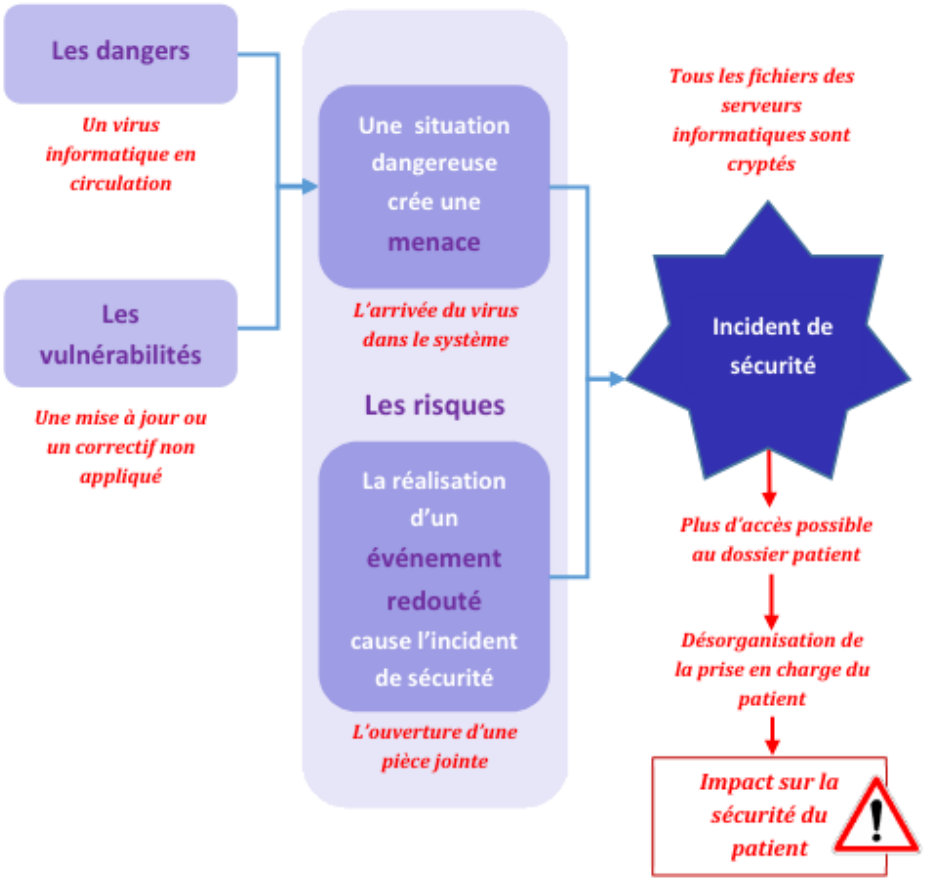
Un risque est un scénario qui combine un événement redouté et une ou plusieurs menaces. Son niveau est réalisé par le croisement de son niveau de vraisemblance et de gravité.

Exemple de cartographie des risques



Document 1.8 : risques liés à l'informatisation des données patient par l'exemple

Extrait du guide pratique de la direction générale de l'offre des soins (DGOS) à destination des directeurs d'établissements de santé.



Tournez la page S.V.P.

Document 1.9 : extrait de la fiche n°3 du guide pratique de la direction générale de l'offre des soins (DGOS) à destination des directeurs d'établissements de santé

La clinique s'appuie sur le guide pratique de la DGOS visant à apporter un éclairage sur les enjeux de la sécurité du système d'information dans un établissement de santé et à exposer aux décideurs quelles sont les bases de la mise en place d'une démarche de sécurité. (*Source social-sante.gouv.fr*›

La fiche n°3 « Définition de la sécurité du système d'information dans les établissements de santé » **présente le fondement d'une démarche sécurité ainsi que les projets majeurs liés à cette démarche.**

Les notions fondamentales de la sécurité

1 - La disponibilité (D) : elle permet de garantir en permanence la communication et l'échange des données de prise en charge des patients, sans défaut y compris pendant les heures non ouvrées.
La disponibilité des SI qui aident à la production des soins doit être au centre des préoccupations sécuritaires des établissements.

Une panne entraîne l'arrêt du DPI – *Etablissement de la région du Limousin* « La panne d'un serveur dont le contrat de maintenance est arrivé à échéance, entraine l'arrêt du DPI. Plus aucun dossier patient n'est accessible »

Un virus bloque la production – *Etablissement de la région du Limousin* « Un virus non détecté par le logiciel anti-virus se propage, rendant inutilisables les postes de travail jusqu'à l'intervention d'un technicien spécialisé »

2 - L'intégrité (I) : les SI doivent garantir que les informations sont identiques et inaltérables dans le temps et l'espace et certifier leur exhaustivité, leur validité et leur cohérence. Ainsi, les données ne doivent pouvoir être modifiées que suivant des processus clairement définis et par des personnes clairement identifiées. Plus la fiabilité de l'information est critique, plus ces critères sont à prendre en compte.

L'objectif d'intégrité est fondamental pour les données médicales ou financières.

Une défaillance provoque des erreurs des dysfonctionnements – *Etablissement de la région Nord Pas de Calais*
« Une mise à jour de l'application DPI (Dossier Patient Informatisé) a provoqué une modification de tous les numéros d'identification des patients, ayant failli entraîner une erreur de prescription médicamenteuse. »
« Des éléments de calcul ont été involontairement modifiés et cela a provoqué des erreurs de paie massives »

3 - La confidentialité (C) : l'information ne doit être accessible qu'aux personnes autorisées. En amont, la réflexion sur la gestion des droits et des accès est essentielle. Seules les personnes ayant besoin de l'information doivent pouvoir y accéder. Plus cette information est « sensible » plus le nombre de personnes doit être réduit.

Des cas divers de divulgation – *Région Nord Pas de Calais*
« Des personnels accèdent aux dossiers médicaux de leur collègue »
« Des personnes extérieures pénètrent dans des bureaux et consultent des dossiers patients »
« L'assistante a laissé par inadvertance des documents de direction sur l'imprimante »
« Un prestataire informatique intervient dans l'établissement et fait la copie de tous les DPI de l'établissement pour disposer de données de test »

4 - La preuve (P) : elle permet l'investigation en cas de dysfonctionnement et d'incidents. Les SI doivent pouvoir fournir la preuve d'un évènement donné et permettre la vérification du bon déroulement des traitements informatiques réalisés par les applications. Les mécanismes généralement employés sont la génération de traces informatiques et un système d'imputabilité qui permet d'associer une action à son auteur.

Absence de preuve – *Région Nord Pas de Calais*
«Une modification illégitime d'un dossier RH a été détectée. Aucun élément ne permet d'identifier l'auteur»

Un des projets majeurs de la démarche est la sécurisation de l'infrastructure et de son exploitation.
Ce projet vise à sécuriser les éléments informatiques (poste de travail, serveurs informatiques, bases de données, bornes wifi, infrastructure réseau de l'établissement, etc.) en appliquant les bonnes pratiques issues de l'état de l'art. La première étape est de rendre redondants certains équipements matériels pour assurer, via des mécanismes de résilience, la disponibilité du système d'information en cas de panne de ces équipements.

Dossier documentaire n° 2 : spécifique à la partie 2A

Document 2.1 : plan d'adressage du réseau de la clinique

Le plan d'adressage est le suivant :

RÉSEAU	ADRESSE
Services libéraux	172.20.0.0/16
Laboratoire	172.21.0.0/16
Clinique XYZ	172.22.0.0/16
Radiologie	172.23.0.0/16
CMCO	172.24.0.0/16
DMZ	192.168.10.0/24
Serveurs	10.20.30.0/24

Document 2.2 : serveurs de la clinique CMCO

Nom des serveurs	Fonction	Adresse IP
serv-ldap	Serveur *Windows server* 2019	10.20.30.11
serv-dns	Serveur *Windows server* 2019	10.20.30.11
serv-dhcp	Serveur *Windows server* 2019	10.20.30.11
serv-syslog	Serveur de journaux système Syslog	10.20.30.12
serv-vpn	Serveur de réseaux privés virtuels VPN	10.20.30.13
serv-cloud	Serveur *cloud* interne	10.20.30.14
appli-anes	Application des anesthésistes	10.20.30.15
srv-web	Site web de la clinique	192.168.10.2

Document 2.3 : description de l'application *Web* APPLI-ANES

La clinique dispose d'une application *Web* métier indispensable au travail des anesthésistes. Cette application se nomme APPLI-ANES et se situe sur un serveur *Web* d'adresse IP 10.20.30.15. L'adresse réticulaire (DNS) de cette application est **appli-anes.cmco.fr**.

Cette application se doit d'être hautement disponible. Actuellement, seule une procédure en mode dégradé concernant cette application est écrite dans le plan de continuité d'activités (PCA).
On peut lire dans ce dernier que, par exemple, comme pour l'ensemble des applications, en cas de coupure, les versions « papiers » des documents de production sont à disposition dans le service.

Le serveur se présente sous la forme d'une machine virtuelle avec les caractéristiques suivantes :

Processeur : Intel Xeon E5
RAM : 2 Go
Serveur de bases de données : mysql server 5.7
Le serveur dispose d'une seule adresse IP et l'intégration dans le DNS est fonctionnelle.
L'adresse IP est obtenue par une réservation sur le serveur DHCP.

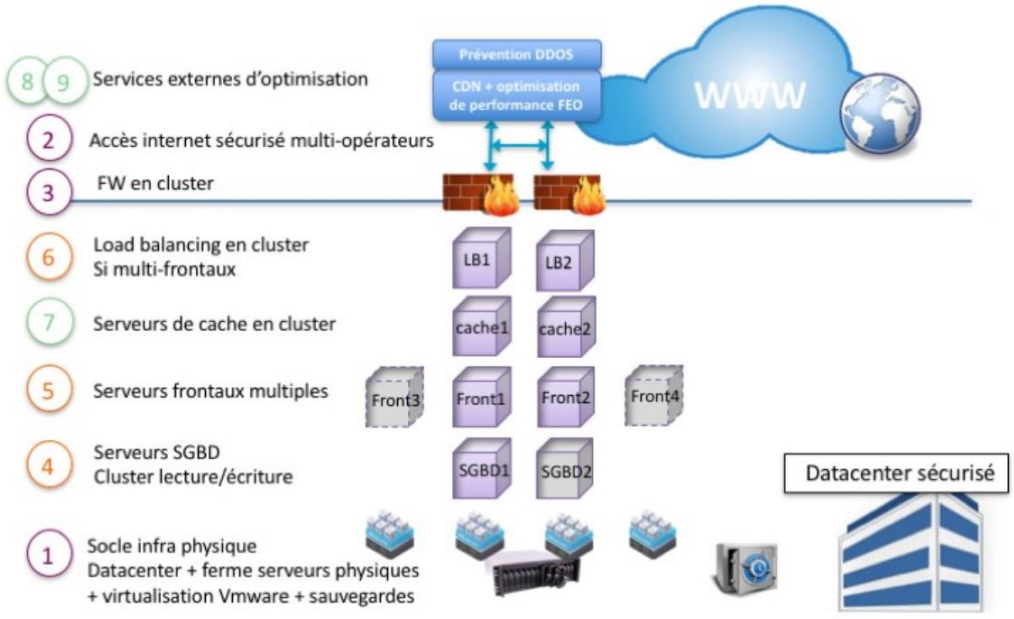
Document 2.4 : le pare-feu Stomrshield Network Security

Le pare-feu de la gamme *Stomrshield Network Security* installé :

- permet de filtrer les accès entre les différents réseaux et pour accéder à internet. La politique de sécurité est celle du “tout interdit par défaut”. La configuration permet de limiter l’accès aux besoins strictes des différents réseaux virtuels (VLAN). L’accès à internet est très utilisé pour des diagnostics à distance et pour des accès à d’autres cliniques via des réseaux privés virtuels (VPN) au standard IPSec ;
- est pourvu d’un filtrage applicatif. Après déchiffrement à l’aide du protocole SSL, le flux HTTP est alors filtré afin d’empêcher l’accès à certaines catégories de sites *Web* comme les sites contenant des logiciels malveillants (*malwares*) ou des sites avec du contenu pornographique ;
- embarque un système de prévention des intrusions (IPS) qui :
    - exploite les bases de signatures d’attaques connues, créées et mises à jour par les équipes de veille sécurité *Stormshield* ;
    - réalise une analyse complète des flux à la recherche de tout comportement réseau anormal, bloquant ainsi de nombreuses attaques de façon proactive, avant même qu’elles ne soient connues et publiées (attaques *zero-day*) ;
- embarque également l’antivirus *ClamAV*. Cet antivirus est également activé sur le filtrage des flux réseaux. Il permet d’empêcher une partie des logiciels malveillants d’accéder aux machines des différents réseaux virtuels (VLAN).

Document 2.5 : projet concernant la disponibilité de l'infrastructure

La clinique désire renforcer la redondance de son infrastructure physique en s'inspirant (avec d'éventuelles simplifications) du modèle suivant :



Un socle technique sécurisé et scalable

1. **Plateforme de virtualisation en datacenter ,** pour déployer les serveurs virtuels du site en haute disponibilité 24/7 et apporter de la scalabilité
2. **Accès internet sécurisé** redondé multi opérateurs
3. **Firewall en cluster** pour sécuriser les accès

Haute disponibilité N1

4. **Serveur de SGBD séparé des frontaux web** , en cluster si besoin, pour + de sécurité et de performance
5. **Serveurs web frontaux multiples** pour absorber le flux de sessions et transactions en parallèle
6. **Load balancer en cluster** pour répartir la charge entre les frontaux

Haute disponibilité N2 + performance optimisée

7. **Serveurs de cache** pour absorber le trafic et distribuer les medias, soulagent les frontaux web
8. **CDN et accélération,** réduit le besoin de bande passante, optimise la délivrance du contenu, accélère la réponse du site
9. **Prévention des attaques Ddos ,** protection contre les attaques Ddos en amont de l'infrastructure

Source : https://www.alfa-safety.fr/hebergement-web/architecture-web-haute-disponibilite-haute-performance

Pour assurer la disponibilité des applications, la clinique a mis en place une solution de virtualisation comprenant 3 serveurs et 2 réseaux de stockage (SAN) avec duplication synchrone pouvant accueillir dans d'excellentes conditions une trentaine de machines virtuelles.

Chaque serveur présente les caractéristiques suivantes :

- dernière génération des processeurs Intel Xeon E5
- 256 Go de RAM
- Disque dur SSD 12 To avec RAID 10
- Unités d'alimentation et de refroidissement écoénergétiques et redondantes.

Les sauvegardes se réalisent hors site.

La direction des systèmes d'information (DSI) souhaite configurer des outils permettant de mettre en place de la tolérance de panne et de l'équilibrage de charge sur les services les plus essentiels.

Tournez la page S.V.P.

Document 2.6 : haute disponibilité en informatique, définition concrète et conseils pratiques

D'après https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1445286-haute-disponibilite-en-informatique-definition-concrete-et-conseils-pratiques/

En informatique, la haute disponibilité (*High Availability* –HA-) permet d'assurer et de garantir la bonne organisation des applications ou services procurés, et ce, 24h/24 et 7j/7, quelle que soit l'organisation. Elle concerne la répartition de charge et la tolérance aux pannes.

Qu'est-ce que la haute disponibilité en informatique ?

La haute disponibilité (HA) anticipe les difficultés que pourrait rencontrer un internaute. Cela permettra de mettre en place des actions et des paramètres techniques, pour qu'une infrastructure informatique soit toujours en mesure de répondre à la requête d'un utilisateur.

Cela est possible en appliquant certaines règles, comme la sauvegarde, la répartition de la charge, la réplication des données, la redondance, etc., pour restreindre l'indisponibilité d'un système d'information. À notre époque, c'est un investissement essentiel pour qu'une entreprise puisse accroître et fonctionner : le système d'information doit être fiable et disponible.

Si ce n'est pas mis en place, il y a des risques de perte de rendement, de matériels, ce qui pourrait même engendrer des coûts supplémentaires (liés aux pannes, aux moyens à déployer, etc.).

Comment assurer la haute disponibilité d'une infrastructure informatique ?

Pour assurer correctement la haute disponibilité d'une infrastructure informatique, il existe des procédures à mettre en place.

Une architecture en répartition de charge (*Load Balancing*) permet de partager les flux entrants sur de nombreux équipements. Cela donne le temps de localiser une surcharge ou un dysfonctionnement, lors d'un excédent de connexions simultanées ou pendant un pic de trafic. Les requêtes sont ainsi réparties de manière intelligente vers des serveurs moins surchargés.

La tolérance aux pannes (*FailOver*) consiste à rediriger un internaute vers un serveur de secours lorsque le serveur principal ne fonctionne pas. Cela permet aux administrateurs système de chercher et de corriger la panne. Le but de ce dispositif est de pouvoir délivrer un service en continu sans que l'utilisateur en soit lésé.
Pour sécuriser davantage une infrastructure informatique, des sauvegardes régulières éviteront tout risque de pertes de données.

Comment mesurer la haute disponibilité ?

La dénomination haute disponibilité n'a de sens que si l'on détermine la façon de la mesurer. L'utilisateur et le fournisseur doivent se mettre d'accord sur ce que représente la disponibilité et comment le temps est calculé. Les sites informatiques, de leur côté, estiment la haute disponibilité en pourcentage du temps de disponibilité des systèmes.

En règle générale, ce pourcentage de disponibilité est calculé ainsi : X = (n-y) x 100/n.
« n » représente le total des minutes, dans un mois calendaire, et « y » est égal au total des minutes durant lesquelles le service est accessible, durant un mois calendaire. Pour que le calcul soit exact, il faut en exclure les temps d'immobilisation planifiés, les heures de maintenance planifiées ainsi que des exécutions de forces majeures.

Document 2.7 : techniques améliorant la disponibilité

D'après : https://fr.wikipedia.org/wiki/Haute_disponibilit%C3%A9

De nombreuses techniques sont utilisées pour améliorer la disponibilité :

- la redondance des matériels et la mise en grappe (*cluster*) ;
- la sécurisation des données : technologie RAID (ou technologie assimilée) ;
- la possibilité de reconfigurer le serveur « à chaud » (c'est-à-dire lorsque celui-ci fonctionne) ;
- mode dégradé ou un mode panique ;
- plan de secours ;
- et sécurisation des sauvegardes : externalisation, centralisation sur site tiers.

La haute disponibilité exige le plus souvent un local adapté : alimentation stabilisée, climatisation sur plancher, avec filtre à particules, service de maintenance, service de gardiennage et de sécurité contre la malveillance et le vol. Attention aussi au risque d'incendie et de dégât des eaux. Les câbles d'alimentation et de communication doivent être multiples et enterrés. Ils ne doivent pas être saillants dans le parking souterrain de l'immeuble. Ces critères sont les premiers à entrer en compte lors du choix d'un prestataire d'hébergement (cas de la location d'un local à haute disponibilité).

Pour chaque niveau de l'architecture, pour chaque composant, chaque liaison entre composants, il faut établir :

- **Comment détecter une panne ?** Exemples : Tests de vie de type "TCP *Health Check*" implémenté par un boîtier, programme de test invoqué périodiquement (« *heartbeat* »), interface de type « diagnostic » sur les composants.
- **Comment le composant est-il sécurisé, redondé, secouru, etc ?** Exemples : serveur de secours, cluster système, stockage RAID, sauvegardes, double attachement SAN, mode dégradé, matériel non utilisé libre prêt à être réinstallé.
- **Comment désire-t-on enclencher la bascule en mode secours / dégradé** ? Manuellement après analyse ? Automatiquement ?
- **Comment s'assurer que le système de secours reparte sur un état stable et connu ?** Exemples : on repart d'une copie de la base et on réapplique les archives, relance depuis un état connu.
- **Comment l'application redémarre sur le mécanisme de secours.** Exemples : redémarrage de l'application, activation d'un mode dégradé, reprise de l'adresse IP du serveur défaillant par le serveur de secours.
- **Comment reprendre éventuellement les transactions ou sessions en cours** ? Exemples : persistance de session sur le serveur applicatif, mécanisme pour assurer une réponse à un client pour une transaction qui s'est bien effectuée avant défaillance mais pour laquelle le client n'a pas eu de réponse.
- **Comment revenir à la situation nominale** ? Exemples :
    - si un mode dégradé permet en cas de défaillance d'une base de données de stocker des transactions en attente dans un fichier, comment les transactions sont-elles ré-appliquées quand la base de données redevient active ;
    - si un composant défaillant a été désactivé, comment s'effectue sa réintroduction en service actif (nécessité par exemple de resynchroniser des données, de retester le composant, etc.).

Dossier documentaire n° 3 : spécifique à la partie 2B

Document 3.1 : RadiOne - Solution applicative de MediSoft

Depuis 20 ans déjà, l'entreprise de services du numérique (ESN) MediSoft fait partie des principaux éditeurs de systèmes d'information en France.
La société MediSoft s'est développée sur le marché de l'informatique des cabinets de radiologie avec son logiciel principal RadiOne. Cette entreprise française s'engage à améliorer la performance des soins pour ses clients.

Le groupement des cliniques du Nord (GCN) est un client de MediSoft et utilise RadiOne pour ses services de radiologie.

RadiOne est une solution unifiée, réunissant l'ensemble des applications et informations administratives, financières et médicales utiles au radiologue et à ses équipes.
Multi-sites et multi-activités, la solution RadiOne s'adapte à toutes les typologies d'organisations.
RadiOne permet de piloter les cabinets en temps réel, de simplifier et de sécuriser leur gestion. Elle améliore la productivité et l'organisation à coûts maîtrisés. Elle permet d'évaluer et de faire progresser la qualité du service rendu au patient.

RadiOne est « 100 % *Web* » et offre la possibilité aux cabinets de radiologie d'alléger considérablement les équipements et les coûts associés à leurs infrastructures informatiques.

Mobilité et ouverture pour une disponibilité permanente, facilité d'administration et sécurité maximisée, permettent de bénéficier d'un service optimal.

Document 3.2 : MediSoft - Hébergeur de données de santé

Dans le cadre de la procédure de certification des hébergeurs de données de santé (HDS), MediSoft a officiellement obtenu la certification HDS.

MediSoft est certifié sur les 6 activités sur lesquelles peut être un hébergeur :

- la mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
- la mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
- la mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
- la mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
- l'administration et l'exploitation du système d'information contenant les données de santé ;
- la sauvegarde de données de santé.

Document 3.3 : RadiOne - Extrait du schéma relationnel de la base de données clients de MediSoft

Cette base de données est utilisée par MediSoft pour héberger les données de santé de ses clients, dont le groupement de cliniques du nord et notamment la clinique CMCO.

Client (IdClient, RaisonSocialeClient, AdresseClient, CPClient, VilleClient, TelephoneClient, CourrielClient)
Clé primaire : IdClient

Site (IdSite, IdClient, NomSite, AdresseSite, CPSite, VilleSite)
Clé primaire : IdSite, IdClient
Clé étrangère : IdClient en référence à IdClient de la relation Client

Salle (IdSalle, IdSite, IdClient, NomSalle, DescriptionSalle)
Clé primaire : IdSalle, IdSite, IdClient
Clé étrangère : (IdSite, IdClient) en référence à (IdSite, IdClient) de la relation Site

Appareil (IdAppareil, IdSalle, IdSite, IdClient, NomAppareil, DateMiseEnService, DateProchaineMaintenance)
Clé primaire : IdAppareil, IdSalle, IdSite, IdClient
Clé étrangère : (IdSalle, IdSite, IdClient) en référence à (IdSalle, IdSite, IdClient) de la relation Salle

DossierMedical (IdDossierMedical, IdPersonne, DateDossier)
Clé primaire : IdDossierMedical
Clé étrangère : IdDossierMedical en référence à IdDossierMedical de la relation DossierMedical
Clé étrangère : IdPersonne en référence à IdPersonne de la relation Personne

Examen (IdExamen, IdDossierMedical, CodeCPAM, DateExamen, CompteRenduExamen, IdAppareil)
Clé primaire : IdExamen
Clé étrangère : IdDossierMedical en référence à IdDossierMedical de la relation DossierMedical
Clé étrangère : IdAppareil en référence à IdAppareil de la relation Appareil

PratiquerExamenMedical (IdPratique, IdPersonne, IdExamen)
Clé primaire : IdPratique
Clé étrangère : IdPersonne en référence à IdPersonne de la relation Personne
Clé étrangère : IdExamen en référence à IdExamen de la relation Examen

Personne (IdPersonne, IdSite, IdClient, Role, SpecialiteMedecin, CodeSecu, Nom, Prenom, Adresse, CP, Ville, Telephone, Mail, Mutuelle)
Clé primaire : IdPersonne, IdSite, IdClient
Clé étrangère : (IdSite, IdClient) en référence à (IdSite, IdClient) de la relation Site

Remarques :

- Le champ *Role* est un caractère permettant de distinguer parmi les personnes, les patients (‘P’), le personnel médical (‘M’) et le personnel administratif (‘A’).
- Le champ *SpecialiteMedecin* n’est renseigné que pour le personnel médical.

Document 3.4 : RadiOne - Extrait du patron de conception modèle-vue-contrôleur (MVC)

RadiOne est une solution développée en programmation orientée objet (POO), selon le modèle MVC. Cette application interagit avec la base de données clients de MediSoft.

Contrôleurs :

- Connexion.php
- ControleurPrincipal.php
- Deconnexion.php
- DetailExamens.php
- ListePraticiens.php
- MonProfil.php
- Recherches.php

Modèle :

- Administratif.php
- Appareil.php
- DossierMedical.php
- Examen.php
- Medecin.php
- Administratif.php
- Personne.php
- Personnel.php
- Salle.php
- Site.php

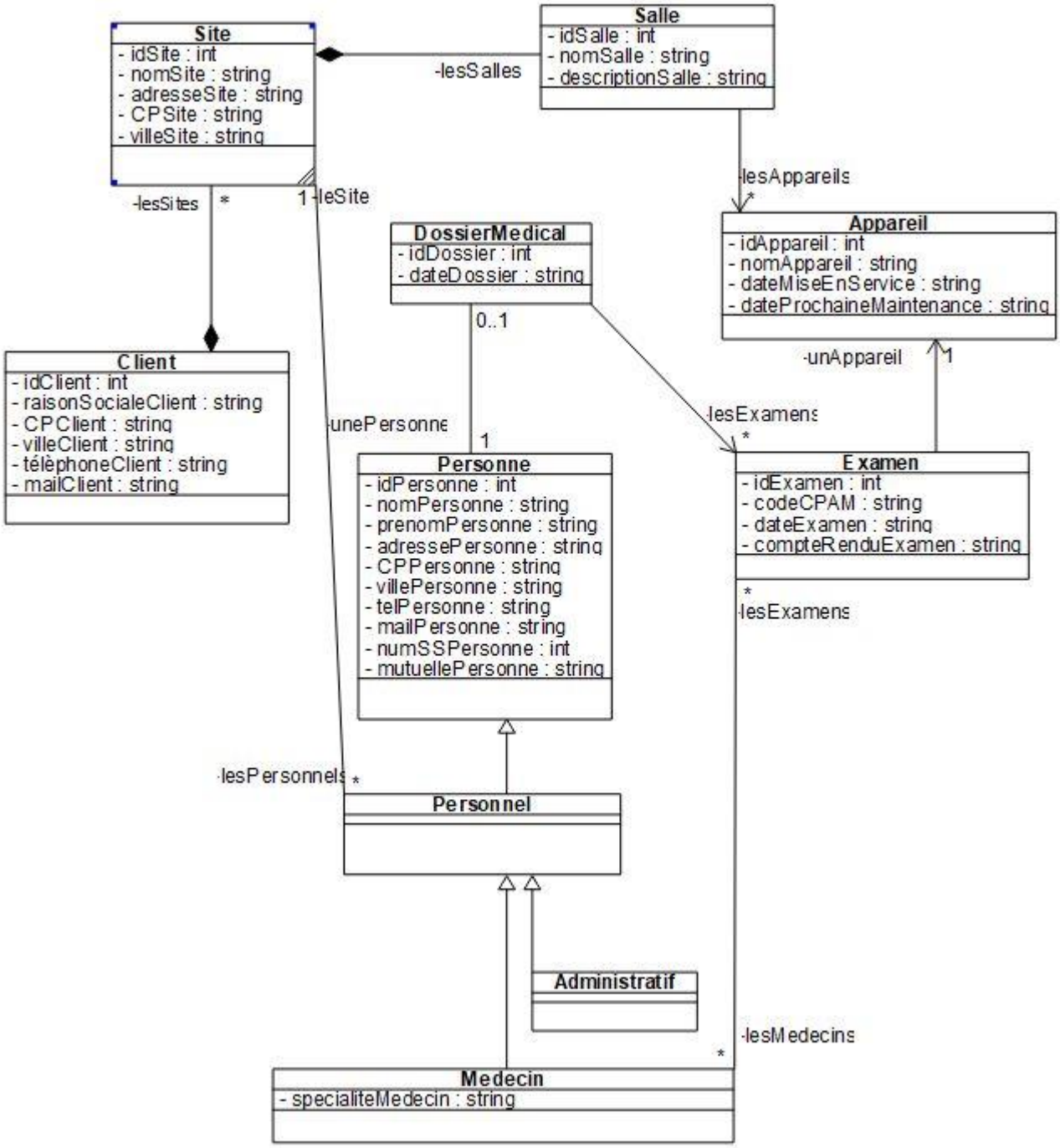
Vues :

- Authentification.php
- ConfirmationAuth.php
- Deconnexion.php
- DetailExamens.php
- Entete.php
- ListePraticiens.php
- ListeSpecialites.php
- MonProfil.php
- Pied.php
- Recherches.php

Tournez la page S.V.P.

Document 3.5 : RadiOne - Extrait du diagramme de classes métier

Légende	
———	Association, navigabilité bidirectionnelle
——→	Association, navigabilité monodirectionnelle
——▷	Héritage (correspond à la tête de flèche non pleine)
——◆	Composition



Document 3.6 : RadiOne - Extrait de la classe d'accès aux données PdoClients

```php
<?php
/* Classe d'accès aux données, qui utilise les services de la classe PDO */

class PdoClients{
        private static $serveur='mysql:...';
        private static $bdd='dbname=Clients';
        private static $user='...' ;
        private static $mdp='...' ;
        private static $monPdo;
        private static $monPdoClients=null;

/* Constructeur crée l'instance de PDO */
    private function __construct(){
        PdoClients::$monPdo = new PDO(PdoClients::$serveur.';'.PdoClients::$bdd,
                                      PdoClients::$user, PdoClients::$mdp);
        PdoClients::$monPdo->query("SET CHARACTER SET utf8");
    }
/* Fonction statique qui crée l'unique instance de la classe */
    public  static function getPdoClients(){
        if(PdoClients::$monPdoClients==null){
            PdoClients::$monPdoClients= new PdoClients();
        }
        return PdoClients::$monPdoClients;
    }
/* Retourne toutes les spécialités des médecins d'un site d'un client */
    public function getLesSpecialites($site, $client){
        $req = "select distinct SpecialiteMedecin as specialite from Personne
            where IdSite='$site' and IdClient='$client'
            and Role='M' order by SpecialiteMedecin";
        $res = PdoClients::$monPdo->query($req);
        $lesLignes = $res->fetchAll();
        return $lesLignes;
    }
/* Retourne tous les praticiens d'une spécialité d'un site d'un client */
    public function getLesPraticiens($site, $client, $specialite){
        $req = "select * from Personne where IdSite='$site'
            and IdClient='$client' and SpecialiteMedecin='$specialite'";
        $res = PdoClients::$monPdo->query($req);
        $lesLignes = $res->fetchAll();
        return $lesLignes;
    }
}
?>
```


Tournez la page S.V.P.

Document 3.7 : RadiOne - Maquette de recherche de spécialistes

Document 3.8 : RadiOne - Maquette de connexion

Document 3.9 : Top 10 des failles de sécurité des applications *Web*

Source owasp.org

L'organisation *Open Web Application Security* (OWASP) est un organisme à but non lucratif mondial qui milite pour l'amélioration de la sécurité des logiciels. L'objectif est d'informer les individus ainsi que les entreprises sur les risques liés à la sécurité des systèmes d'information. L'organisation fonctionne comme une communauté de professionnels qui partagent une vision commune.

L'OWASP publie un classement qui recense les failles de sécurité les plus critiques.

Ce qui a changé dans le top 10 pour 2021 : il y a trois nouvelles catégories, quatre catégories avec des changements de nom et de portée, et une certaine consolidation.