Initier les bonnes pratiques en matière de sécurité dans mon organisation

Jeudi 15 avril 2021

Christian Viallon

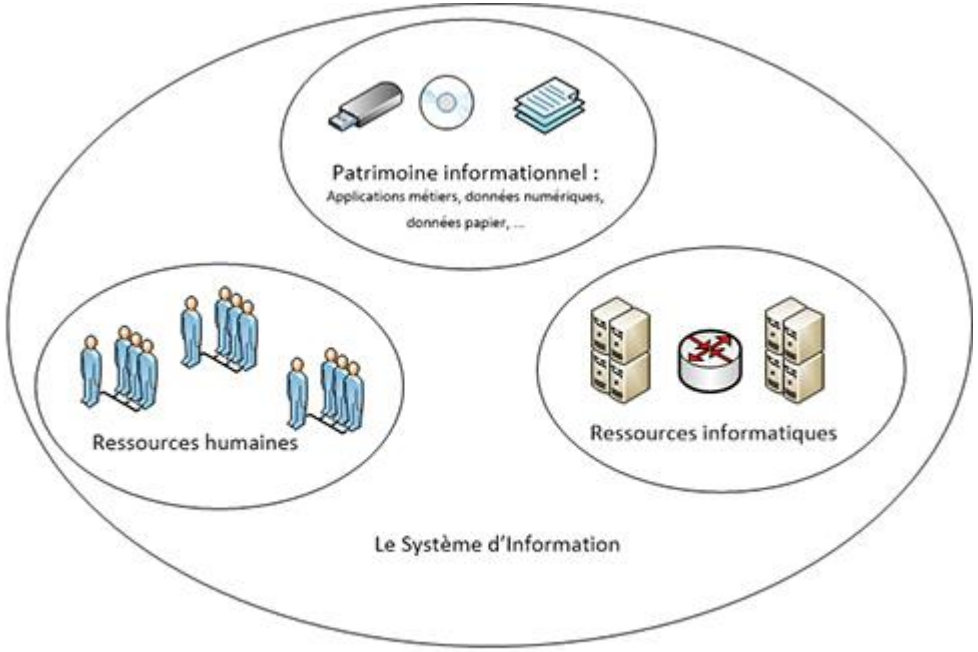
La sécurité du système d'information

2

De quoi s'agit-il ?

RAPPEL : QU'EST-CE QU'UN SYSTÈME D'INFORMATION ?

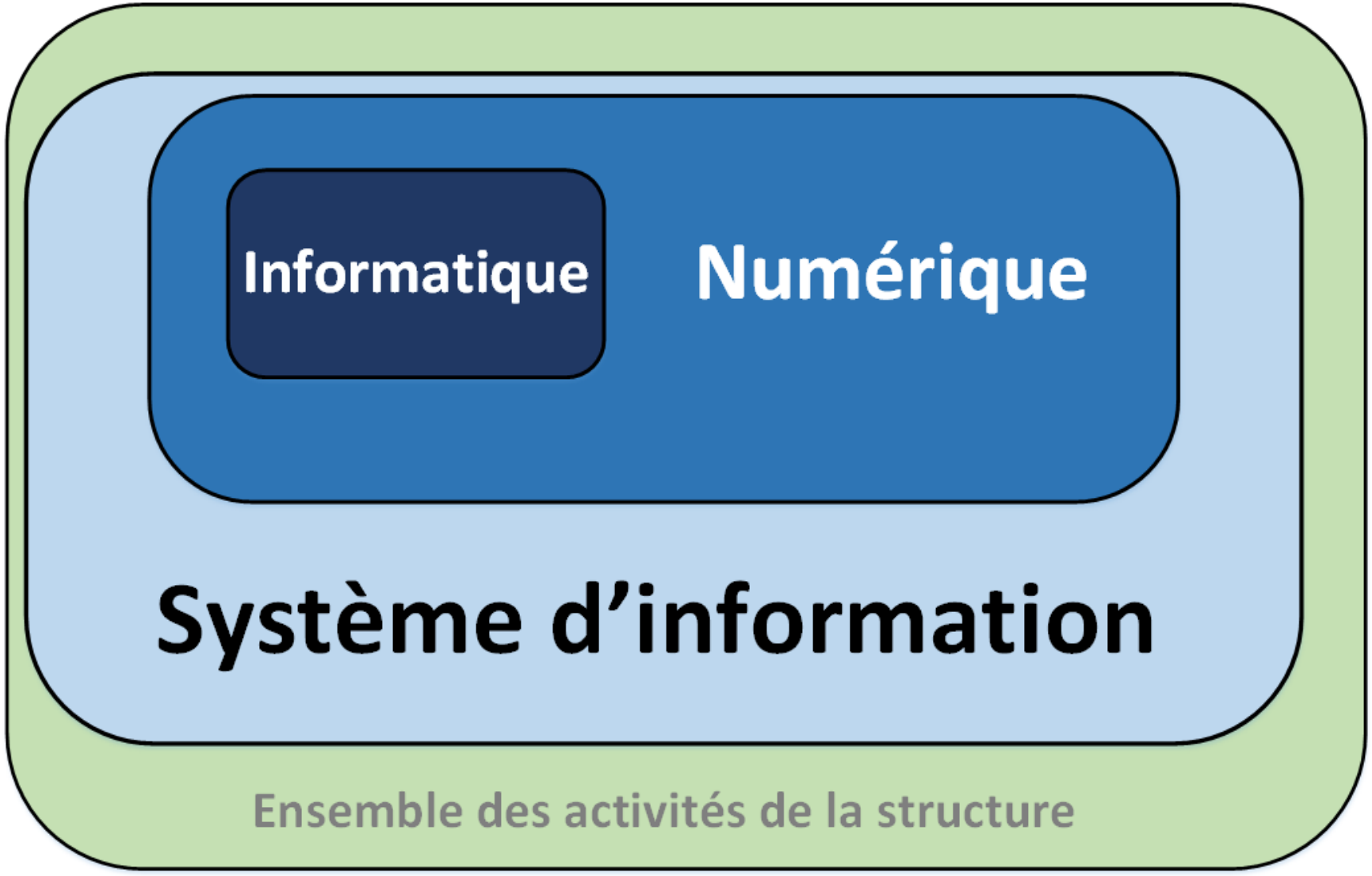
- Un système d'information (SI) est un ensemble organisé de ressources : matériels, logiciels, humaines, données et procédures qui permet de collecter, regrouper, classifier, traiter et diffuser de l'information dans les organisations. (Christophe Legrenzi)



Les composantes du Système d'Information

Schéma très fortement inspiré des présentations et formations de Denis Virole (Société Agéris) et Jean Louis-Brunel (Pôle national SSI de l'Education nationale)

RAPPEL : LE SI CE N'EST PAS QUE L'INFORMATIQUE !



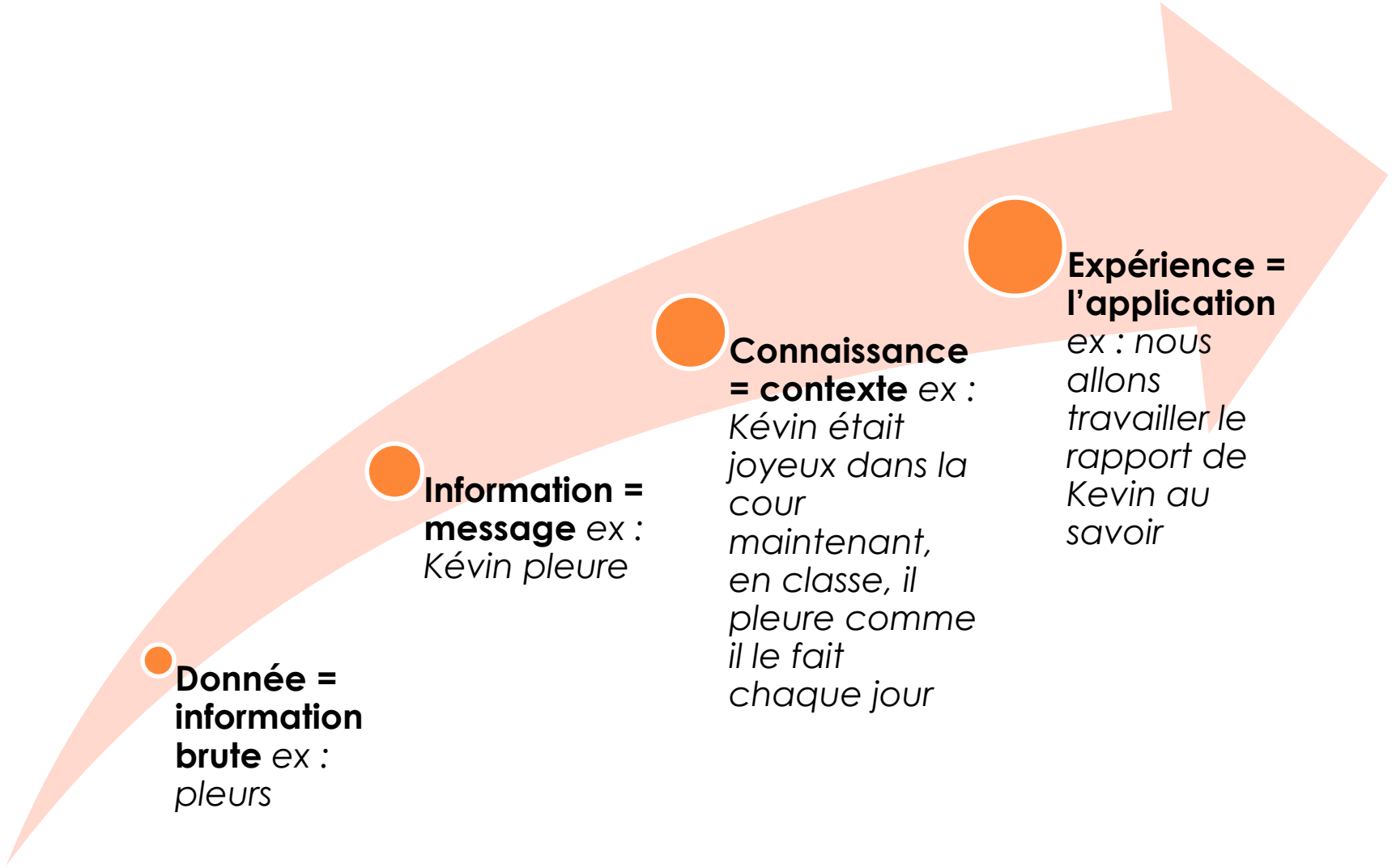
 D'après Legrenzi-Gapaillard, les nouveaux schémas directeurs des SI

La sécurité du système d'information (SSI)

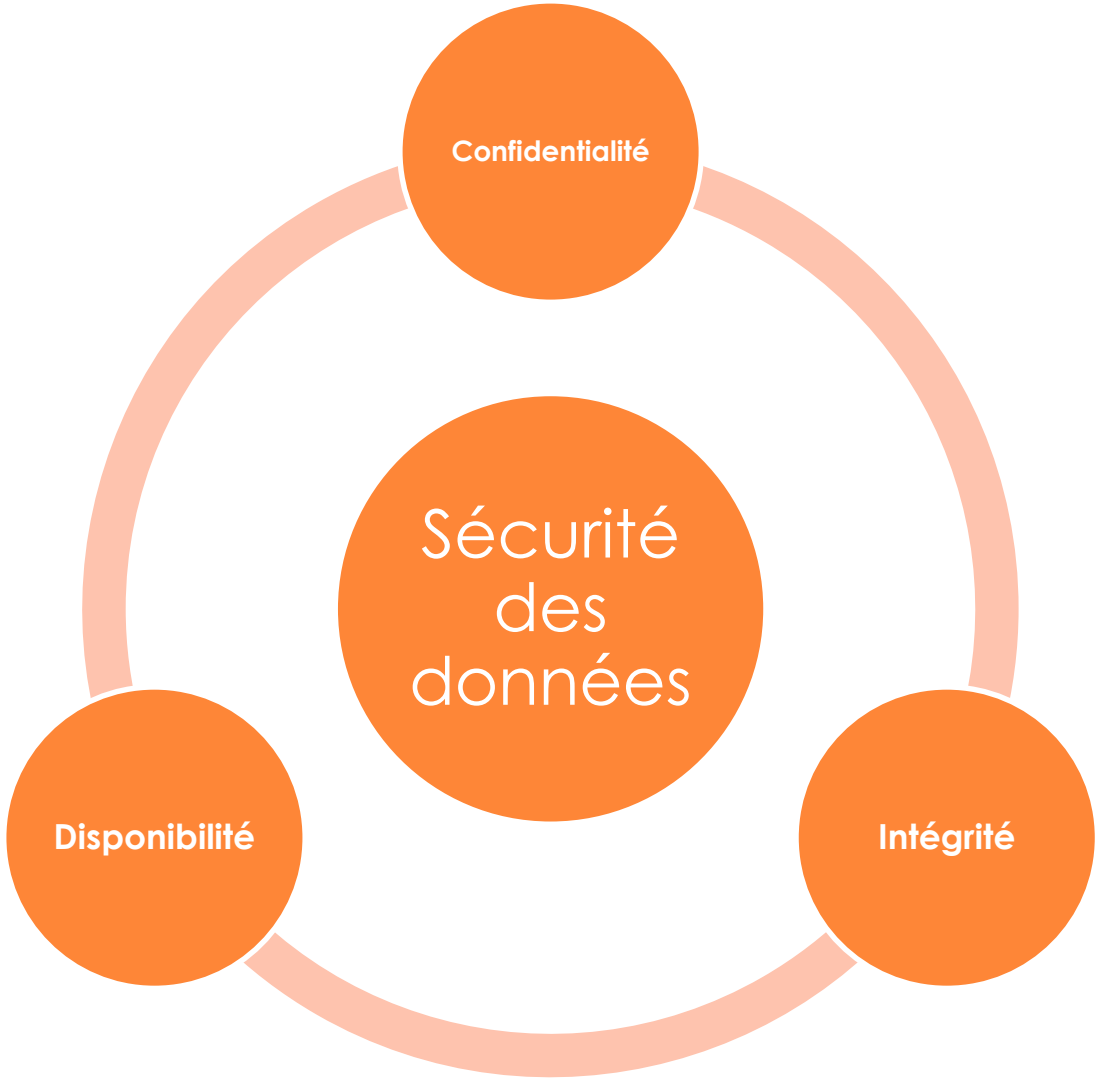
- La **sécurité informatique** est l'ensemble des règles, procédures techniques et outils utilisés pour préserver la confidentialité, l'intégrité et la disponibilité des données traitées par les systèmes informatiques.
- La **Sécurité du Système d'Information (SSI)** couvre un champ plus large :
  - à la sécurité informatique la SSI ajoute les composantes **humaines** et **informationnelles** du Système d'Information,
  - ainsi que la sécurité de **l'information « non numérique »** sous forme de document papier, de savoir, etc.
- **Deux questions** à se poser :
  - qu'est-ce que je veux protéger ?
  - pourquoi je veux ou je dois le protéger ?

LA SÉCURITÉ DES DONNÉES

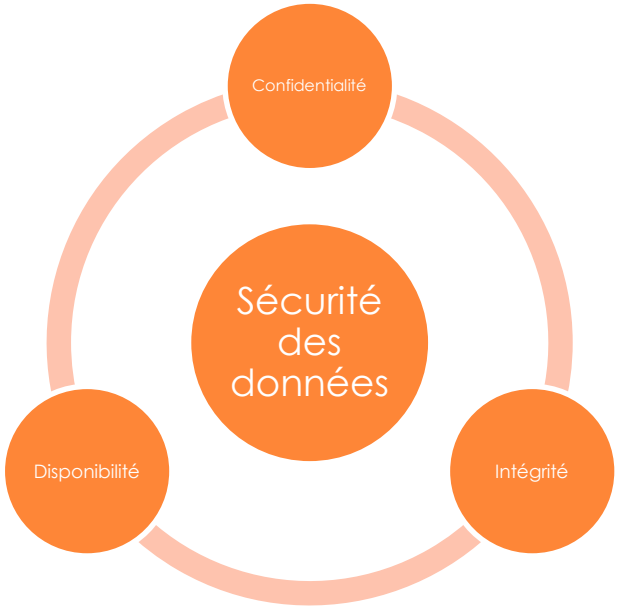
Donnée – information – connaissance -expérience



LA TRIADE *INTÉGRITÉ – CONFIDENTIALITÉ – DISPONIBILITÉ* *NORME ISO/CEI 27001*



LA TRIADE *INTÉGRITÉ – CONFIDENTIALITÉ - DISPONIBILITÉ*



- **Intégrité** : les données sont authentiques et n'ont pas été modifiées par mégarde ou malveillance pendant le traitement, le stockage ou la transmission.
- **Confidentialité** : prévenir l'accès non autorisé aux données et aux équipements utilisés pour leur traitement et prévenir l'utilisation non autorisée de ces données et de ces équipements.
- **Disponibilité** (souvent associée à la résilience) : tout ce qui permet d'assurer la continuité du service de traitement.

La hiérarchie des normes juridiques

Exemple du dossier de l'usager et RGPD

Droit « dur »

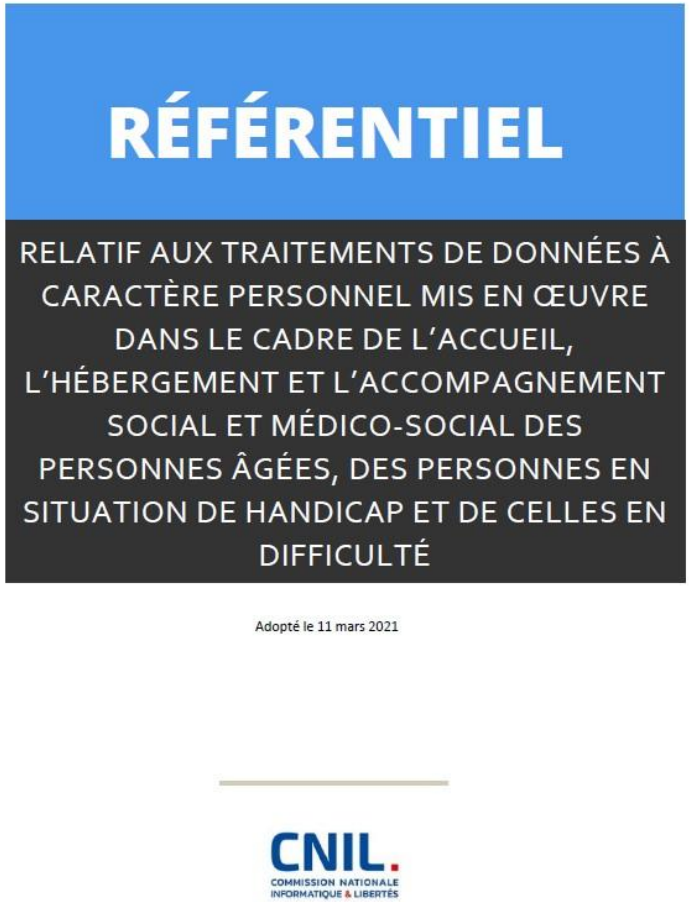
- Code du Patrimoine
- Code des Relations entre le Public et l'Administration
- Code de la Santé Publique
- Code de l'Action Sociale et des Familles

Droit « souple »

- Les normes
- Les lignes directrices (CEPD)
- Les référentiels (CNIL)
- Les Codes de Conduite

DROIT SOUPLE : LE RÉFÉRENTIEL « SOCIAL » CNIL

- Un outil d'aide à la mise en conformité pour permettre d'appliquer les règles de protection des données aux traitements relevant du secteur social et/ou médico-social.
- Ce référentiel n'a pas de valeur contraignante.
- Site CNIL https://www.cnil.fr/fr/publication-du-referentiel-pour-la-prise-en-charge-medico-sociale-personnes-agees-handicap-difficulte
- FAQ CNIL https://www.cnil.fr/fr/questions-reponses-referentiel-suivi-medico-social-des-personnes-agees-handicap-difficulte



Droit souple : la suite de normes ISO/CEI 27000

- Une **famille** comprenant pas moins d'une douzaine de normes relatives à la sécurité des systèmes d'information .
- La plus connue est l'**ISO/CEI 27001**. Publiée en octobre 2005 et révisée en 2013, son titre est "Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences". Elle permet de certifier des organisations.
- La ISO 27001 est fondée sur la **gestion des risques**. Il s'agit :
  - d'identifier les **informations sensibles** ou **précieuses**,
  - identifier les **menaces** dont elles pourraient être l'objet,
  - mettre en place les mesures permettant de **contrôler chaque risque**.
- La norme définit les exigences pour la mise en place d'un **système de management de la sécurité de l'information** (SMSI).
- Elle est organisé en 4 phases : établir, implémenter, maintenir, améliorer.

Droit dur et droit souple : la politique générale de sécurité des systèmes d'information de santé (PGSSI-S)

- Mise en place par l'Etat la PGGSSI-S est un **cadre** pour :
  - aider les porteurs de projet dans la **définition des niveaux de sécurité** attendus,
  - permettre aux industriels de **préciser les niveaux de sécurité** proposés dans leurs offres,
  - accompagner les structures de santé dans la définition et la mise en œuvre de leur **politique de sécurité des SI**.
- Elle est composée de **référentiels** et de **guides** pratiques (https://esante.gouv.fr/securite/pgssi-s/espace-de-publication) se présentant avec une notion de paliers : un palier minimal et des paliers progressifs, permettant aux porteurs de projet d'améliorer progressivement la sécurité de leurs projets.
- Le champ d'application de la PGSSI-S est défini à l'article L1110-4-1 du **code de la santé publique**. L'article L1110-4-1 est **opposable**.

La PGSSI-S en quelques mots

Suis-je concerné (e) ?

Acteur du domaine de la santé

Médico-social

Social

OBLIGATION DE DÉCLARER À L'ARS

- Art L 1111-8-2 du CSP : « Les établissements de santé, les organismes et services exerçant des activités de prévention, de diagnostic ou de soins et les établissements médico-sociaux **signalent sans délai** aux autorités compétentes de l'État et au groupement d'intérêt public mentionné à l'article L. 1111-24, dans des conditions fixées par décret, **les incidents significatifs ou graves de sécurité des systèmes d'information**. »
- Les catégories d'incidents et conditions de mise en œuvre du signalement des incidents graves de sécurité des systèmes d'information sont décrites dans les articles D. 1111-16-2 à D. 1111-16-4 du CSP. Il s'agit des :
  - incidents ayant des conséquences potentielles ou avérées sur la **sécurité des soins**;
  - incidents ayant des conséquences sur la confidentialité ou **l'intégrité** des données de santé;
  - incidents portant atteinte au **fonctionnement normal** de l'établissement, de l'organisme ou du service.

L'HÉBERGEMENT DES DONNÉES DE SANTÉ

- CSP Art. L1111-8 « Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article »
- Certification HDS cf. https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante
- La question de la certification HDS se pose dès lors que l'on fait appel à
  - Un **hébergeur d'infrastructure physique** (activités 1 et 2)
  - Un **hébergeur infogéreur** (activités 3 à 6).

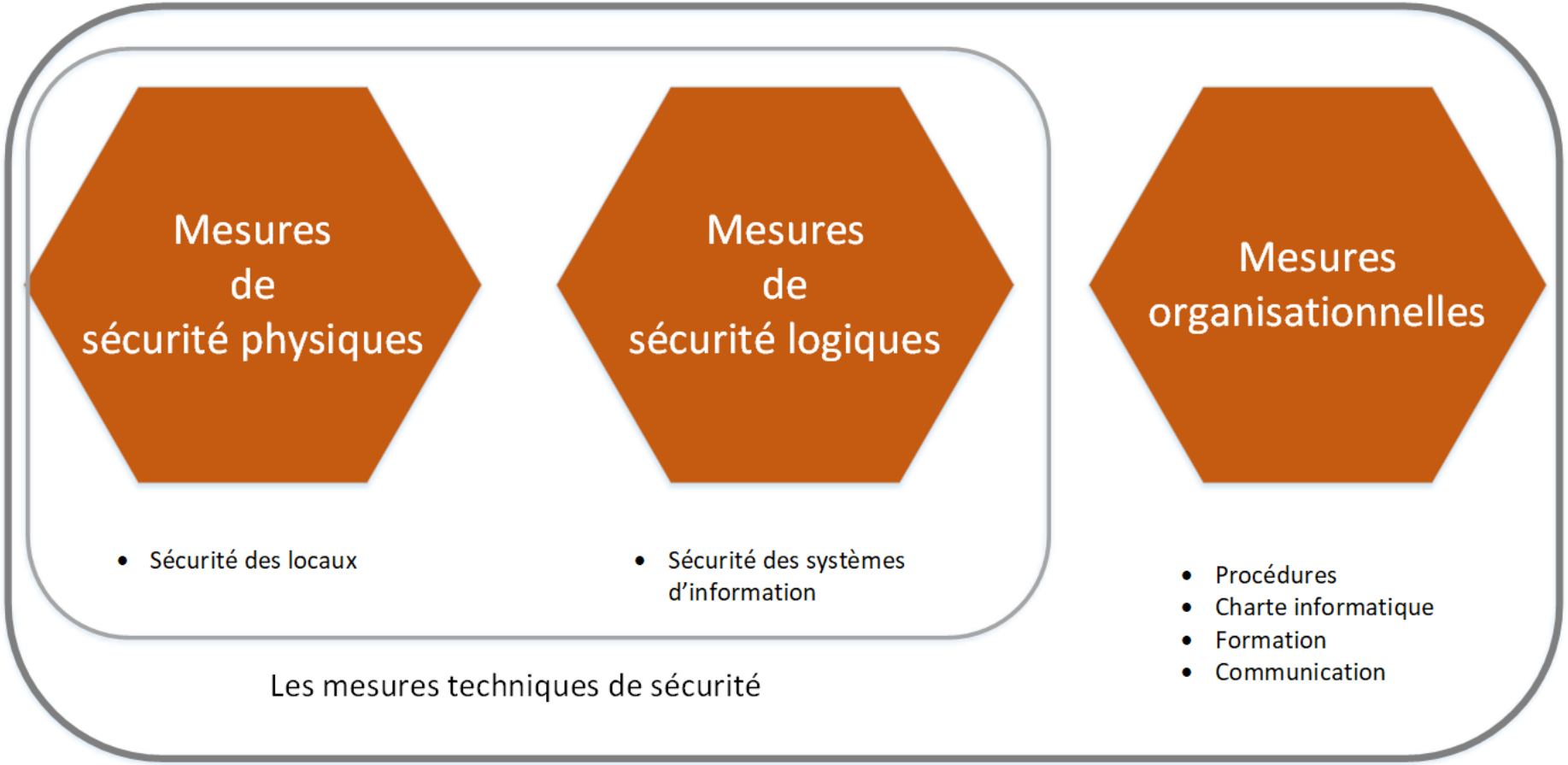
Les 6 activités du périmètre d'obligation HDS

1. 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 ;
2. 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 ;
3. 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 ;
4. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
5. *L'administration et l'exploitation du système d'information contenant les données de santé ;*
6. La sauvegarde des données de santé.

Depuis le 2 avril 2019 l'activité 5 a été retirée du périmètre d'obligation (en attente de concertations voir Doctrine technique).

La sécurité des données s'appréhende de façon globale

Appréhender la sécurité de façon globale



Les mesures générales de sécurité

D'après Gérard Haas

QU'EST-CE QUE LA SÉCURITÉ ORGANISATIONNELLE ?

Reportage de TF1 : la préparation (hautement sécurisée) des sujets du Bac

QU'EST-CE QUE LA SÉCURITÉ ORGANISATIONNELLE ?

Reportage de TF1 : la préparation (hautement sécurisée) des sujets du Bac

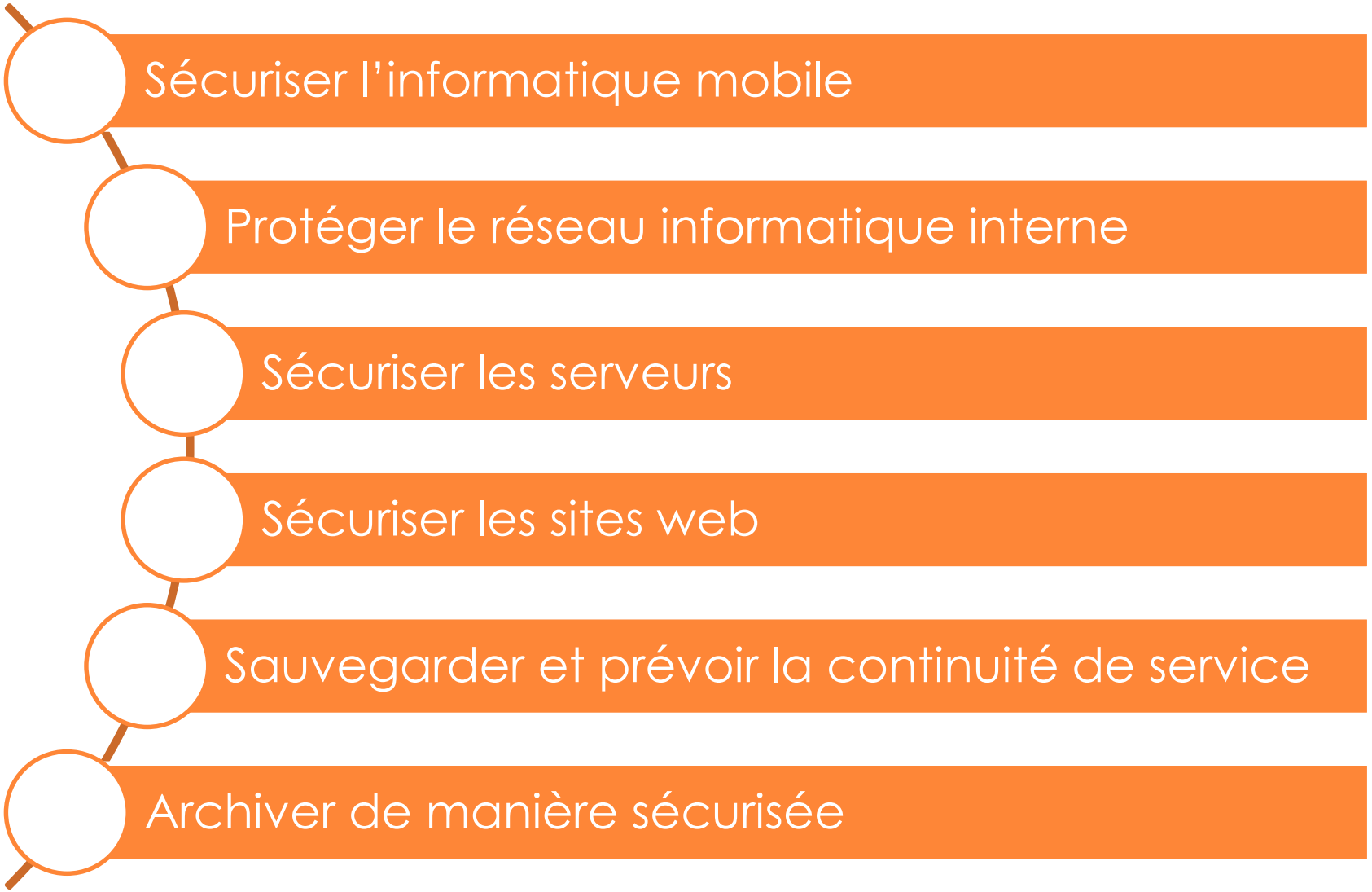
METTRE EN ŒUVRE LA POLITIQUE DE SÉCURITÉ

22

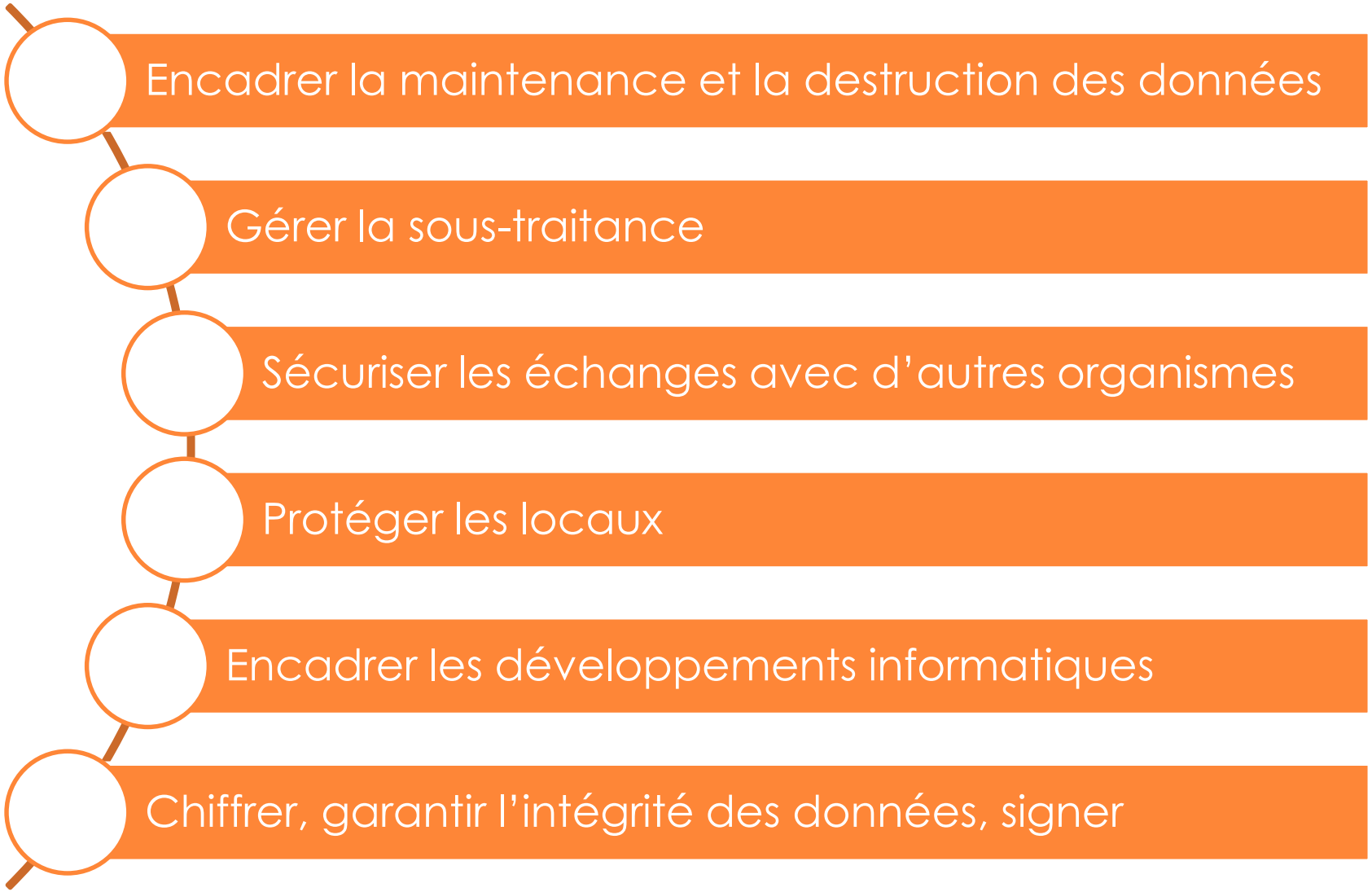
Démarche en 16 mesures proposée par la CNIL

Mesures 1 à 5

Mesures 6 à 11



Mesures 12 à 16



La checklist de la CNIL

	FICHES	MESURE	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	☐
		Rédigez une charte informatique et donnez lui une force contraignante	☐
2	Authentifier les utilisateurs	Définissez un identifiant (login) unique à chaque utilisateur	☐
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	☐
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	☐
		Limitez le nombre de tentatives d'accès à un compte	☐
3	Gérer les habilitations	Définissez des profils d'habilitation	☐
		Supprimez les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	☐
		Informez les utilisateurs de la mise en place du système de journalisation	☐
		Protégez les équipements de journalisation et les informations journalisées	☐
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	☐
5	Sécuriser les postes de travail	Prévoyez une procédure de verrouillage automatique de session	☐
		Utilisez des antivirus régulièrement mis à jour	☐
		Installez un « pare-feu » (*firewall*) logiciel	☐
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	☐
		Faites des sauvegardes ou des synchronisations régulières des données	☐
		Exigez un secret pour le déverrouillage des smartphones	☐
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	☐
		Sécurisez les accès distants des appareils informatiques nomades par VPN	☐
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	☐
8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installez sans délai les mises à jour critiques	☐
		Assurez une disponibilité des données	☐

	FICHES	MESURE	
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	☐
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	☐
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	☐
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	☐
		Stockez les supports de sauvegarde dans un endroit sûr	☐
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	☐
		Prévoyez et testez régulièrement la continuité d'activité	☐
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	☐
		Détruisez les archives obsolètes de manière sécurisée	☐
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	☐
		Encadrez par un responsable de l'organisme les interventions par des tiers	☐
		Effacez les données de tout matériel avant sa mise au rebut	☐
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des sous-traitants	☐
		Prévoyez les conditions de restitution et de destruction des données	☐
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	☐
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	☐
		Assurez-vous qu'il s'agit du bon destinataire	☐
		Transmettez le secret lors d'un envoi distinct et via un canal différent	☐
15	Protéger les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	☐
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	☐
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	☐
		Évitez les zones de commentaires ou encadrez-les strictement	☐
		Testez sur des données fictives ou anonymisées	☐
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	☐
		Conservez les secrets et les clés cryptographiques de manière sécurisée	☐

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

MÉTHODOLOGIE

PRIVILÉGIER L'APPROCHE PAR LE RISQUE

EVALUATION DES RISQUES

Sources de risques

- Identifier
- Qualifier la capacité de chaque source

Evènements redoutés

- déterminer l'impact sur la vie privée
- estimer la gravité

Menaces

- identifier les menaces
- leur source vraisemblable

Risques

- déterminer le niveau de chaque risque
- gravité
- vraisemblance
- cartographie

d'après HAAS AVOCATS

Analyser l'impact (préalablement)

Analyse d'Impact relative à la Protection des Données

Menace

Risque

Mesures correctives

juridiques

Techniques

Elevé mais traitement indispensable

Transmission à la CNIL pour avis

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Risque Résiduel ?

Acceptable ou nul

Mise en oeuvre du traitement

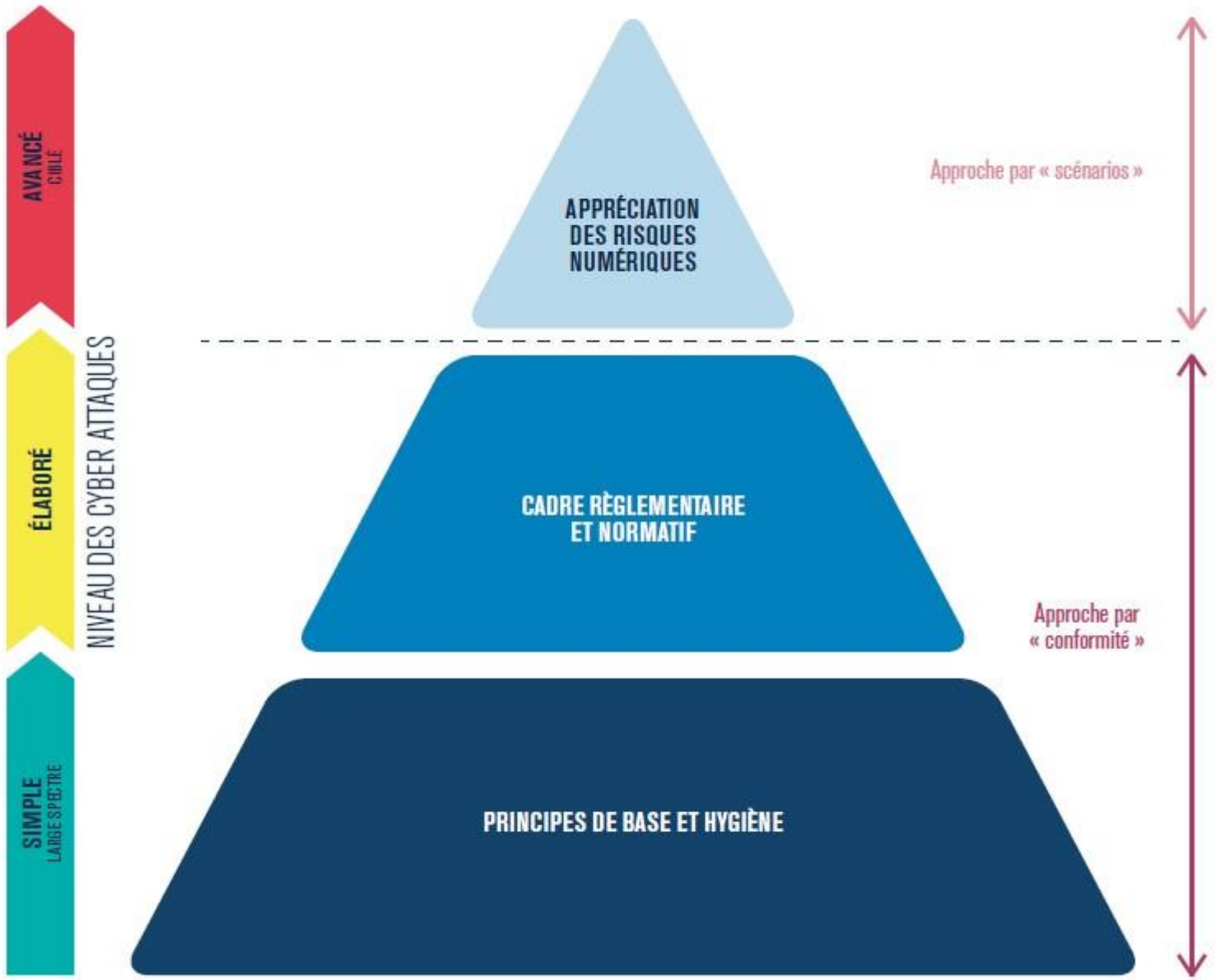
Elevé

Abandon du traitement

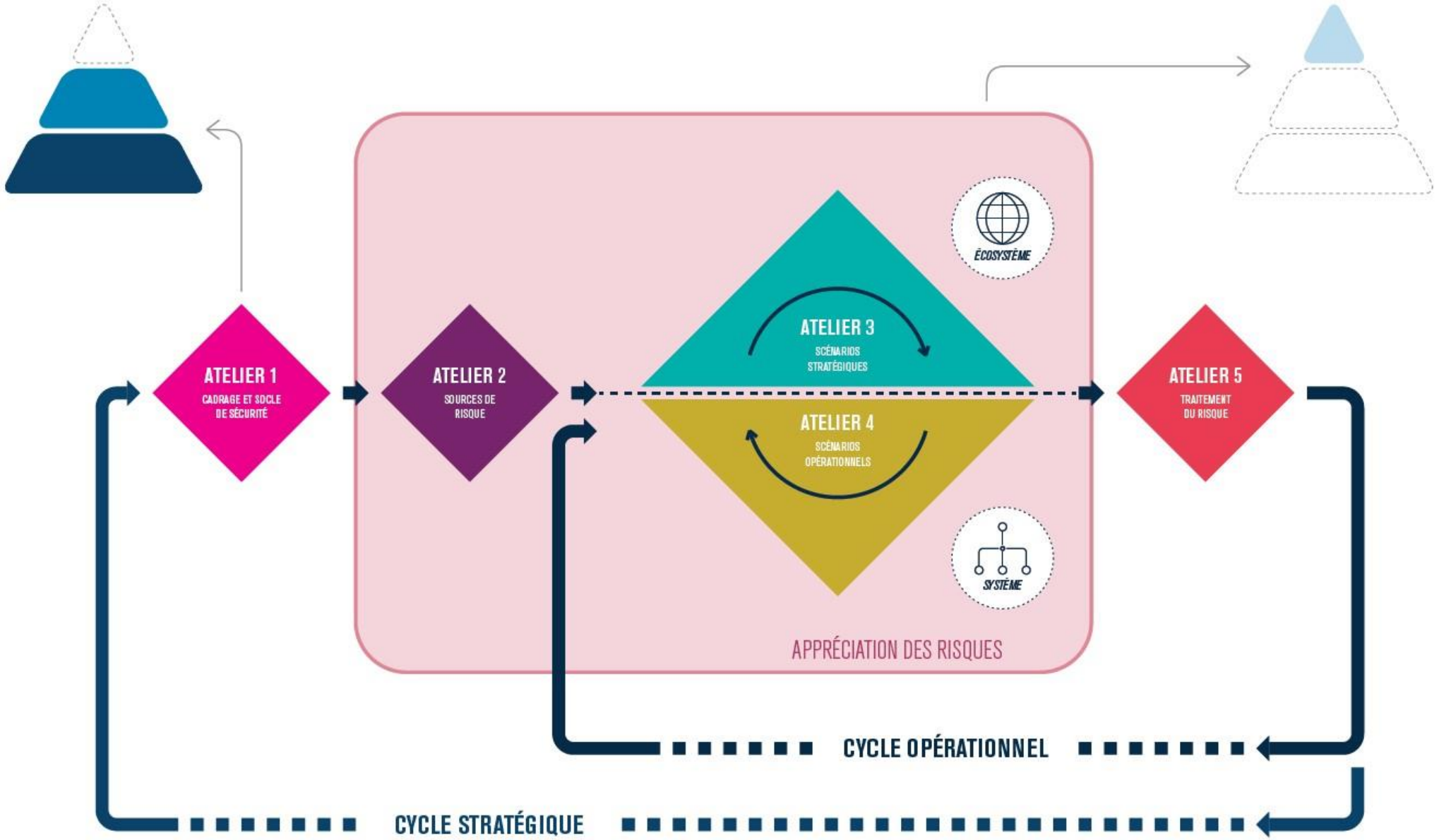
La méthode EBIOS Risk Manager

- EBIOS est la méthode **d'appréciation** et de **traitement** des **risques numériques** publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) avec le soutien du Club EBIOS.
- EBIOS adopte une approche de management du risque numérique partant du plus haut niveau (grandes missions de l'objet étudié) pour atteindre progressivement les fonctions métier et techniques, par l'étude des scénarios de risque possibles.
- La méthode EBIOS RM peut être utilisée à plusieurs fins :
  - mettre en place ou renforcer **un processus de management du risque** numérique au sein d'une organisation ;
  - **apprécier** et **traiter les risques** relatifs à un projet numérique, notamment dans l'objectif d'une homologation de sécurité ;
  - définir **le niveau de sécurité** à atteindre pour un produit ou un service selon ses cas d'usage envisagés et les risques à contrer, dans la perspective d'une certification ou d'un agrément par exemple.

EBIOS PYRAMIDE DU MANAGEMENT DU RISQUE NUMÉRIQUE



EBIOS UNE DÉMARCHE ITÉRATIVE EN 5 ATELIERS



DANS LA BOÎTE A OUTILS DE LA SÉCURITÉ

Quelques procédures et documents indispensables

- Charte d'utilisation du système d'information
- Charte de la politique de confidentialité (et la suite de documents d'information qui en découle).
- Procédures :
  - Procédure d'accès et d'exercice des droits,
  - Procédure de création d'un traitement,
  - Procédure d'archivage,
  - Procédure relative à l'analyse de l'impact sur la protection des données personnelles,
  - Etc.
- Référentiel de sécurité

UN OUTIL NEXEM – RESSOURCIAL : LE RÉFÉRENTIEL DE SÉCURITÉ

RESSOURCIAL

nexem
employeurs, différemment

Référentiel sécurité

Référentiel de Sécurité

Nom de l'organisme

Cliquez ou appuyez ici pour entrer du texte.

Action	Date	Acteur
Rédaction		
Vérification		
Approbation		

UN OUTIL NEXEM – RESSOURCIAL : LE RÉFÉRENTIEL DE SÉCURITÉ

Sécurité physique 7
Inventaire des accès « opp
Sécurisation des accès .....
Système d'alarme .....
Vidéosurveillance.....
Alarme anti-intrusion....
Détecteurs de fumée ....
Procédure de levée de d
Gestion des clés et des bac
Mode de distribution de
Suivi.....
Que se passe-t-il en cas
Organigramme des serrure
Modalités de copie des
Modalités de diffusion e
Sécurité des systèmes élec
DUERP .....
Sécurité logique .....
Organisation de la sécurité de
Organisation .....
Veille .....
Gestion des risq ans les
Mobilité et télétravail .....
La sécurité des ressources
A l'embauche du
Confidentialité et secret
Sensibilisatio
Formation .....
Départ du salarié.....
Gestion des actifs.....
Gestion des supports amovil
Mise au rebut des actifs.....
Contrôle d'accès du système d
Politique des mots de passe
Gestion des droits d'accès ...
Gestion de la continuité d'activité 13
Sécurité organisationnelle .....
Sensibilisation des salariés trai
Cette sensibilisation est
O est la form e
A nme
Le cédures sont es di
Les procédures sont-elles ré
Les procédures sont-elles tr
Les procédures suivantes so
Remarques complémentair
Politique d'archivage .....
Procédure d'archivage .....
L'organisme a défini les modalités de partage de l'information .....
Les dispositions relatives au secret professionnel s'appliquent-elles dans l'organi
Les dispositions relatives au secret professionnel s'appliquent-elles à tout le pers
Si Les dispositions relatives au secret professionnel ne s'appliquent pas un engag
confidentialité est-il requis ? .....
ement fait l'objet : .....
sécurité organisationnelle .....
sécurité organisationnelle est inscrite au Plan de formation de
tes .....
de formations prévues ou réalisées en 2019 .....
Gestion conformité .....
Certifications.....
Revue de conformité .....
Délégué à la protection des données personnelles (DPO) .....
Journal des opérations de collecte .....
Registre des activités de traitement .....
Journal des demandes d'accès .....
Analyses d'impact relative à la protection des données (AIPD) .....
valuation rapide .....

Près de 150 points de contrôle !

RESSOURCES SUR LE SITE DE L'ANAP

- Sécurité des SI des établissements de santé https://ressources.anap.fr/numerique/publication/2570-securite-des-systemes-d-information-des-etablissements-de-sante
- Kit de cybersurveillance à destination des professionnels de santé https://ressources.anap.fr/numerique/publication/2702-kit-de-cybersurveillance-a-destination-des-professionnels-de-sante
- Élaborer une fiche de poste pour un RSSI https://ressources.anap.fr/numerique/publication/2401-elaborer-une-fiche-de-poste-pour-un-rssi
- Guide pratique spécifique pour la mise en place d'un accès Wifi https://ressources.anap.fr/numerique/publication/386-guide-pratique-specifique-pour-la-mise-en-place-d-un-acces-wifi
- Kit SI pour le directeur de structure médico-sociale : http://ressources.anap.fr/numerique/publication/2409
- Fonctions d'un dossier de l'usager à informatiser http://ressources.anap.fr/numerique/publication/2722
- Kit Gestion de projet d'informatisation dans une structure médico-sociale http://ressources.anap.fr/numerique/publication/2144
- Kit Démarche processus http://ressources.anap.fr/numerique/publication/2733-kit-demarche-processus
- Résolution, les communautés de pratiques par l'ANAP https://www.anap.fr/communaute/#undefined_c6152

Ressources sur le site de l'ANS et de la DNS

- Doctrine technique du numérique en santé (version 2020) https://esante.gouv.fr/virage-numerique/doctrine-technique
- Les webinaires de l'ANS : https://esante.gouv.fr/ans/webinaires
- La page du virage numérique sur le site de l'ANS : https://esante.gouv.fr/virage-numerique
- Catalogue des terminologies de santé https://smt.esante.gouv.fr/catalogue-des-terminologies/
- Espace de publication PGSSI-S https://esante.gouv.fr/securite/pgssi-s/espace-de-publication

Ressources sur le site du Collectif SI Médico-social HDF

- Cycle de webinaires : https://www.collectifsims-hdf.net/webinaires/ (inscription/rediffusions)
- Appel à projet ESMS Numérique : https://www.collectifsims-hdf.net/appel-a-projets-programme-esms-numerique/
- Club RSI – DSI : https://www.collectifsims-hdf.net/club-rsi-dsi/

POUR ALLER PLUS LOIN

- Sur la norme 27001 : https://fr.wikipedia.org/wiki/ISO/CEI_27001
- PGSSI https://esante-formation.fr/course/view.php?id=7
- La méthode EBIOS : https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/
- CNIL Sécurité des données https://www.cnil.fr/fr/securite-des-donnees
- CNIL Guide sécurité des données personnelles https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf
- CNIL Référentiel « social et médico-social » https://www.cnil.fr/fr/publication-du-referentiel-pour-la-prise-en-charge-medico-sociale-personnes-agees-handicap-difficulte
- CNIL L'analyse d'impact relative à la protection des données (AIPD) https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

19 rue Marius Grosso
69120 Vaulx-en-Velin
Tél : 06.14.20.26.03
Mail : contact@ressourcial.fr
Web : www.ressourcial.fr
FAQ base documentaire RGPD
http://www.ressourcial.fr/faq-rgpd/
Besoin d'en savoir plus ?
christian.viallon@ressourcial.fr Newsletter hebdomadaire : envoyer un courriel pour s'inscrire.